TODO LO QUE NADIE HA OSADO DECIRTE ANTES

HACKER JOURNAL

www.hacker-journal.com

bimensual – año 2 –

KGB: Mezclar archivos en CD de música

Diálogo con un Hacker socrático

Comparativa: ANTIMALWARE

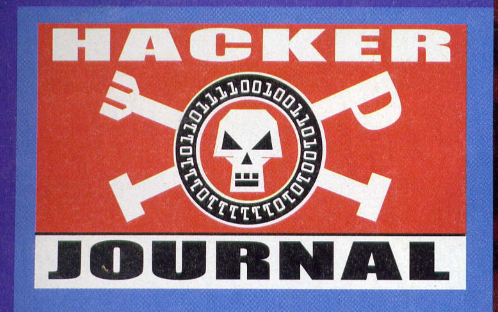
Encuentra al mejor cazador de programas malignos

BLACK HAT DEFCON

La comunidad Hacker a DEBATE

8 414090 031417 00009

4ever



Año 2 - N. 9 - 2004 - Bimensual

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3d0, Eric Sala, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Difusión: Paul-Luc PEREZ

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

LUCES DE ALARMA

En estas páginas encontraréis dos amplios reportajes sobre Black Hat y Defcon 12, dos encuentros de amplia repercusión en el mundo hacker. El primero de ellos tiene un carácter más oficial, mientras que el segundo muestra el espíritu hacker en toda su originalidad. Sin embargo, las ediciones de este año han venido marcadas por el recelo ante la posibilidad de represalias. En efecto, Estados Unidos se encuentra actualmente en fase de "primar la seguridad por encima de cualquier otro concepto". En esencia, ello significa que el gobierno y su policía intervienen de forma preventiva ante todo lo que les puede parecer que sea sospechoso. Sospechoso de lo que sea. La legislación da cobertura a esta caza de brujas revisitada. En consecuencia, las denuncias y juicios por presunto mal uso de la información proliferan como hongos. Y por ello, los expertos en seguridad son cada vez más renuentes a publicar sus hallazgos, si no ya a renunciar a ellos. Corren malos tiempos para la libre circulación de la información y el conocimiento...

De forma imparable, parece que el mismo espíritu va calando en nuestro propio país. Recientemente se ha aprobado una ley que afecta a la informática. En esencia se trata de proteger los derechos de autor, pero el celo de la ley, procedente de legislaturas pretéritas y asumido por la actual sin reparos, puede llegar a conculcar derechos adquiridos y genuinos, como el derecho a realizar copia de seguridad de los programas y contenidos legalmente adquiridos. En los tiempos del reinado del disquete de 3,5 pulgadas, empresas como Adobe obligaban al cliente a volver a comprar su producto si el disquete que le permitía instalar la aplicación sufría daños. El disquete contaba con sofisticadas protecciones, de modo que el usuario pagaba mucho dinero por un precario mecanismo de uso de un programa. Parece que estos tiempos dorados para algunos amenazan con volver.

Se supone que los usuarios de a pie estamos contribuyendo con estos sacrificios no deseados (¿necesarios?) a la paz mundial. Cuesta ver la relación, pero nuestras finanzas se van a enterar.

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS



NEWBIE



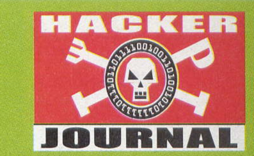
MID HACKING



HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO



02 - Editorial
04 - Correo
06 - Noticias
08 - Black Hack 2004: Conferencia mundial sobre seguridad informática
12 - Comparativa: el mejor antimalware
14 - Solsticio de invierno: Diálogo con el hacker socrático
16 - Libertad de XOR: ¿sigue vigente el copyright tras modificación digital?
18 - Defcon 12: Cita en Las Vegas
22 - Archivos invisibles en Windows: dónde están, qué hacen, por qué son invisibles y cómo acceder a ellos
24 - Wine: Windows en Linux
26 - Dirección enmascarada
28 - Máximo secreto con KGB
30 - Del lenguaje natural al C y viceversa
32 - Cyberenigma: rayas y puntos para los más avispados

SITIO WEB

Con este número también traemos novedades en la web. Ante todo felicitar a los visitantes ya que cada vez somos más los que visitamos la web y se nota. Más noticias, entradas en los foros, más actividad. Otra novedad es el estreno de dos nuevos foros en la sección de programación, uno sobre el lenguaje .NET/Mono y otro sobre programación web en PHP y ASP. Por último hemos iniciado una encuesta sobre sistemas operativos: ¿Que sistema operativo usas? Os animamos a participar.

lacker-journal.com - La revista Hacking española :: Publicación Independiente - Mozilla Firefox

Bookmarks Tools Help

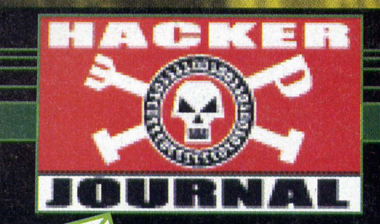
http://www.hacker-journal.com/modules.php?op=modload&name=PNphpBB2&file=index

Forum	Topics	Posts	Last Post
Redaccion			
Redaccion Mensajes de la redacción	2	2	11 Jun 2004 11:49 am Admin
Foro general			
General Opina algo de la revista, cometarios, críticas, sugerencias, artículos, etc	257	1551	30 Sep 2004 12:16 pm Sirik
Seguridad			
Newbie Primeros consejos sobre como podéis hacer más seguro vuestro pc	63	516	25 Sep 2004 12:56 pm Rarok
Pro Sección dedicada a profesionales	21	181	11 Sep 2004 06:45 pm ZaR
Linux Todo sobre Linux	46	267	25 Sep 2004 01:00 pm Rarok
Programación			
General Foro de programación general	10	121	27 Sep 2004 05:42 pm g0lDeN
.NET/Mono Foro de programación en .Net i Mono	0	0	No Posts
PHP/ASP Programando webs dinámicas	0	0	No Posts
Hardware			
General Hardware en general	14	146	29 Sep 2004 04:41 pm Rarok

w.hackerjournalespana.com...

Visita nuestro sitio web:
www.hacker-journal.com

CODIGO DE LA SECRET ZONE
user: 9secret9
password: calei2copio





mailto:

redaccion@hacker-journal.com

SALUDOS DE MONTERREY

hola saludos desde monterrey nuevo leon, mexico
Sólo escribo para felicitarlos por su increible revista y es lo mejor que no tenga publicidad.
Por aca su revista no se encuentra facilmente, quisiera saber como comprar o adquirir su revista?
Espero respuesta por favor,

Francisco Garcia

Gracias por tus felicitaciones, que nos llenan de orgullo. Nos gusta también mantenerla sin publicidad, para no mantener compromisos con nadie más que nuestros lectores. Esperamos que puedas encontrar regularmente Hacker Journal en tu localidad. Desde aquí poco podemos hacer, dependemos en todo de la distribuidora...

...Y DESDE PANAMÁ

Hola soy panameño, no soy hacker pero me parece interesante aprender sobre este mundo, ya no se que hacer con el computador.
Y es interesante buscar errores de seguridad mediante esta práctica. Esto para mi siempre fue un mundo oscuro en el cual nadie sabia ni dava información tan facil, hasta que llegó a mis manos un ejemplar de Hacker Journal.
Me agrado tanto encontrar una revista que hablara de lo que yo quiero aprender, no de los productos que no puedo comprar, fui al mes siguiente a buscar el ejemplar correspondiente a el, y nunca llegó.
Me gustaría saber si hay alguna forma de que yo reciba estas revistas mensualmente en mi apartado postal, de ser así por favor mandar datos sobre trasporte, manejo y costo de la revista por un año.
Se despide de panamá deseándoles que sigan con esa labor, de educar y no pensar que los que estamos aprendiendo los superaremos.
Gracias

THE_MUTANT

¡Gracias a ti, por mandarnos tu enhorabuena desde tan lejos! El espíritu de Hacker Journal es precisamente divulgar conocimientos, e intentar ponerlos al alcance de quienes no los tienen. Lamentamos comunicarte que por el momento no tenemos posibilidad de establecer una suscripción a la revista.

ALGUNOS LÍMITES

La revista es la leche en serio buscaba entretener tiempo y os encontré. Gracias a dios puedo escuhar conversaciones de mi madre aunque sea ilegal no se cree que existe pero weno en fin me han dicho que hay webs en php prefabricadas y quería saber si me podríais pasar alguna o algo. Si puedo colaborar en algo aunque tengo 16 llamar ok enga gracias

Javier

Amigo Javier, nos encanta tu entusiasmo pero tenemos que repetir por enésima vez: ¡no hagáis nada que sea ilegal! De hecho, no queremos que nadie haga nada que simplemente pueda perjudicar a otro. Te recordamos que no se puede escuchar a alguien secretamente. Y aparte de lo que digan las leyes, estamos completamente en contra de espiar a alguien si su permiso. Nos pasamos páginas y páginas hablando de defender la privacidad, de modo que ahora no nos vengáis con lo divertido que es escuchar a alguien sin que lo sepa.
Si buscas webs en PHP prefabricadas las puedes encontrar en la red, por ejemplo buscando en Google por php + web. También puedes explorar paquetes para la creación de sitios web, como PostNuke.

PREGUNTAS Y CUESTIONES

Hola hacker journales. He comprado varios de vuestros numeros, (otros no porque no los pude encontrar), y vuestra revista hermana y la verdad es que me han servido de mucho. Han saciado un poco mis ganas de saber, pero me he quedado con algunas cuestiones. Primero deciros que soy novato en esto y tengo mis limitaciones porque el control que llevan sobre mi en cuanto al PC es exaustivo, para empezar tengo una cuenta limitada en mi propio PC!!!! Bueno pues con eso os quería preguntar algunas cosillas.
Primero si me podéis explicar un poco eso de introducir el CD del 2000 y eso para saltarme el password e instalar por ejemplo el Limewire y su apoyo java.
Luego preguntaros sobre los troyanos. ¿Es possible hacerlos invisibles a los antivirus y firewalls?? ¿Cómo?? (no penseis mal, no soy peligroso, para los PC soy bastante gafe)
Y finalmente si se puede trazar una IP para encontrar exactamente su punto geográfico. Exactamente me refiero como mínimo a ciudad y calles cercanas.
Bueno gracias por todo y felicitaros por esa revista tan buena que "of course" seguiré comprando.
Un saludo:

Devil

Los novatos son tan bienvenidos (o más) como los más veteranos. Todos empezamos como novatos y precisamente la ayuda y la paciencia de otros es lo que permite ir aprendiendo. Visto así, todos somos novatos...
Saltarse un password depende del tipo de password, y de lo que el password esté protegiendo. En las páginas de Hacker Journal hemos hablado sobre cómo saltar algunos de ellos, por ejemplo al arrancar Windows, pero cada protección tiene requisitos distintos. Como buen aprendiz de hacker, tendrás que buscar lo que necesitas...
Los troyanos, como todo tipo de software maligno o malware, es indetectable... hasta que alguien lo detecta. Los antivirus y cortafuegos suelen actualizar con frecuencia sus tablas de reconocimiento de virus, de modo que su actualización a menudo es crucial para que resulten útiles ante las nuevas amenazas que surgen continuamente. Lo mejor es ser muy prudente al abrir contenidos procedentes de si-

tios dudosos, no abrir nada en caso de duda y mantener al día el software de protección. Naturalmente, otra solución es cambiarse a un sistema operativo como Linux, que de por sí es menos proclive a este tipo de ataques.
Respecto al número IP, no puedes llegar sólo con él hasta la mesa donde se encuentra el equipo. Ello es debido, entre otras cosas, a que algunos IP se asignan dinámicamente (por ejemplo cuando se llama mediante un módem). Además se pueden utilizar reenviadores que oculten la dirección original. Cuando la policía tiene que rastrear una dirección IP necesita acudir a los registros de todos y cada uno de los equipos de los proveedores de servicio y reenviadores que haya por el camino. Como estos equipos pueden encontrarse en cualquier lugar del mundo, no suele ser tarea fácil llegar hasta su origen. Para un particular, resulta prácticamente imposible. Lo cual, visto desde el punto de vista del emisor (cuando eres tú quien escribe) proporciona una reconfortante sensación de privacidad, ¿no crees?

CONTACTOS

Ante todo tengan un saludo de mi parte para el Equipo de Hacker-Journal, excelente Web FELICIDADES MUCHACHOS.
Soy un lector asiduo de su web
Les escribo ya que poseo una web, claro no tan cool como la de ustedes y me gustaria poner un banner en mi web de hacker-journal, igualmente publicar algunas informaciones de ustedes, claro respetando los derechos de autor y citando de dónde procede la información.
url: http://www.lancelot29.net
Sin mas que decirles.
Gracias

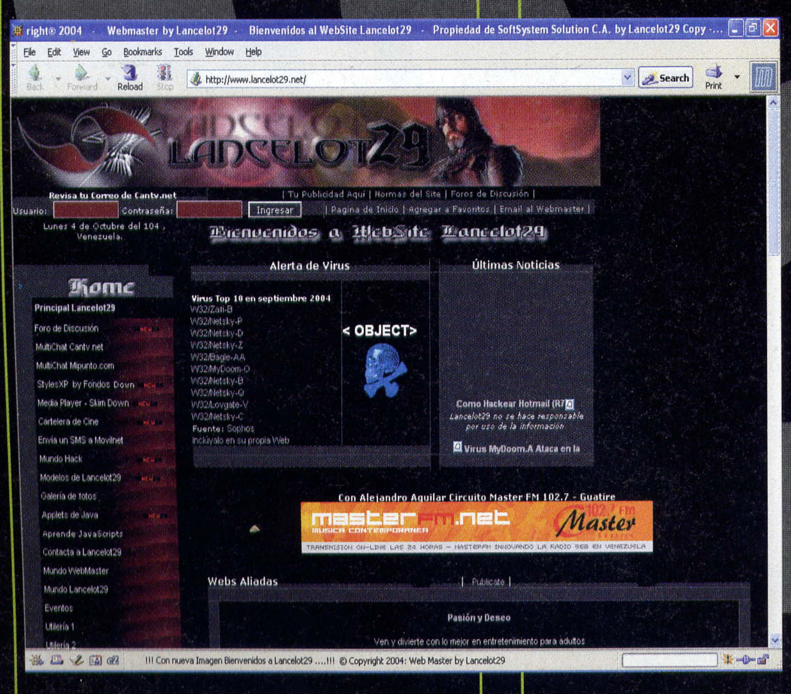
Freddy Garcia

Amigo Freddy, estamos encantados de saber que se nos conocerá también en tu sitio web. Lo hemos visitado y tiene buena pinta. ¡Buena suerte!

SALUDO

Felicitaciones! Tengo la numero uno y la dos de su revista. Que bueno es que puedan tambien tratar sobre temas como los troyanos Subseven, shaolin etc, que son herrmientas que segun he escuchado muy utiles para hackers.
Un saludo desde Sur America, en donde se encuentra tambien la revista de Uds.

ayoria Grec



Gracias por tus ánimos. Nos complace llegar al máximo número de lugares posible.

NUEVA LEY

Hola antes de nada daros la enhorabuena por vuestra revista.
Mi sugerencia es si pudierais dar vuestra opinion sobre la nueva ley que ha entrado en vigor el dia de hoy.Yo la he leido un poco por encima y a mi corto entender, si cualquiera le dice en un foro, como quitar la proteccion a un dvd o como desencriptar un sistema de pago de tv por satelite,cable ,ect ect,aunque sea sin animo de lucro, solamente por compartir conocimientos o investigaciones entre grupos de personas con ansia de saber,te pueden imputar un delito penado con carcel.no estas robando nada solo compartiendo informacion.
gracias por vuestra atencion.salu2

Edu_martinez

El tema es extraordinariamente interesante, en efecto. Tendremos que dedicarle atención a partir de ahora. Es curioso que la ley haya sido aprobada por un gobierno que cuando estaba en la oposición se opuso encendidamente a su aprobación, exactamente con el mismo redactado. ¿A quién favorece en última instancia la nueva normativa? Hay que tener presente que la ley es lo suficientemente abierta como para que los jueces, con su aplicación, fijen los límites de actuación de las diversas acciones que se lleven a cabo. Por otra parte, en Hacker Journal seguimos pensando que vivimos en un estado de derecho y que por lo tanto es imprescindible ser respetuoso con las leyes. Si nos parece que alguna de ellas es abusiva o incorrecta, tenemos todo el derecho como cualquiera a denunciarlo, pero no nos creemos con el derecho de infringirla. Lo que persigue penalizar la ley, aparentemente, es la inducción a cometer delitos informáticos. Y, como siempre, nuestra revista está en contra de toda acción ilegal. Seguiremos informando.

ENIGMA

Acá os dejo un Cyberenigma de un nivel muy básico.
"matemáticamente, en esta frase se encuentran ocho a, más una".

put0pdr0

¡Es un cyberenigma muy bueno! ¡A ver quién más se anima a enviarnos sus logros!

¡HOT!

¡TOM Y JERRY, LOS FAVORITOS!

Pues sí, porque según una encuesta reciente llevada a cabo por el canal de televisión infantil Boomerang, la gran mayoria de los encuestados, con edades comprendidas entre los 25 y los 54 años, respondieron que el personaje animado con el que más han disfrutado ha sido Tom y Jerry.
Tom y Jerry superaron a personajes como Scooby Doo, Don Gato y los Picapiedra.
"Los animales con características humanas son una combinación invencible", dijo el director del canal Boomerang, Dan Balaam. Y realmente pocos personajes humanos llegaron a la lista, inundada de gatos, perros, ratones, correcaminos, coyotes...
Como curiosidad, apuntar que Tom y Jerry aparecieron en las pantallas de televisión en 1940 en un capítulo llamado "El gatito recibe la patada", y el gato sin suerte conocido ahora como Tom se llamaba Jasper.

El Top 10

1. Tom y Jerry
2. Scooby Doo
3. Dangermouse
4. Don Gato
5. Los Picapiedra
6. Bugs Bunny
7. Popeye
8. El Correcaminos
9. Los Autos Locos
10. Hong Kong Phooey

Top 5 Virus

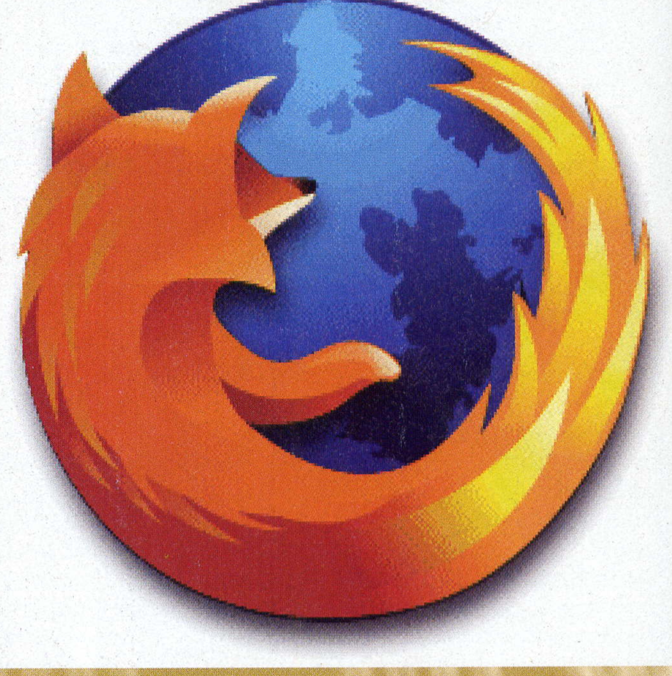
1. Downloader.GK	9,04%
2. Netsky.P	2,36%
3. Gaobot.gen	2,13%
4. Mhtredir.gen	2,08%
5. Sasser.ftp	1,81%

Nuevos top

Bagle.BB	28 Setiembre
HardFull.A	26 Setiembre

De todos es sabido que los virus proliferan continuamente. Por ello, resulta especialmente indicado saber cuáles son los de mayor difusión, para tomar las medidas especiales oportunas de cara a protegerse de invasiones no deseadas.

NUEVO FIREFOX 1.0 PR



Mozilla Firefox se está consolidando poco a poco como uno de los mejores navegadores del mercado y un poderoso competidor del omnipresente Microsoft Internet Explorer.
La fundación mozilla pretendía al publicar la nueva versión, 1.0 PR, de este navegador superar el millón de descargas en diez dias. Curiosamente no sólo se consiguió superar ese récord sino que se hizo en tan sólo cuatro días.
Entre las novedades más importates de esta version destacamos: el LiveBookmarks, un lector de feeds (RSS,Atom,etc) que te crea una carpeta en tus bookmarks con los enlaces a los posts que se incluyen en el feed; una remodelación muy completa de la barra de búsquedas y un instalador de plugins automatizado que incluye una lista de sitios donde accede automaticamente para buscar el instalador e instalar.
Hay que comentar que Firefox es también software libre así que es gratuito. Las alternativas de software gratuito contra las soluciones propietarias y costosas no cesan de mejorar; y en Internet, el proceso se acelera.
Si aún no has probado firefox entra en www.mozilla.org/firefox.

DISCO ÓPTICO CON CAPACIDAD DE TERABYTES



Ha sido duante la Asia-Pacific Data Storage Conference 2004 donde físicos de la Universidad Imperial de Londres han presentado un disco que podría albergar con facilidad la vida de Homer Simpson. Y es que aunque parezca mentira, trescientos cincuenta capítulos de Los Simpson, con un total de ocho mil ochenta minutos de cinta, se podrían grabar facilmente en el interior de un disco de estas excepcionales e innovadoras características.
La tecnología en cuestión, llamada MODS (Multiplexed Optical Data Storage), puede llegar a albergar un Terabyte (mil veinticuatro Gigabytes) de información o su equivalente en vídeo, unas cuatrocientas setenta y dos horas, en un solo disco del tamaño de un CD o DVD.
El disco de 1TB puede grabarse por los dos lados y también a dos capas. Pero nos bastaría con una sola cara y capa de uno de estos discos para guardar trece veces la película del Señor de los Anillos o los doscientos treinta y ocho episodios de Friends.
Aunque todavía faltan algunos años para que la tecnología MODS se encuentre disponible en el mercado, se estima que entre 2010 y 2015 se convertirá en una realidad tangible. Antes llegarán las tecnología de discos ópticos como Blue-Ray, que tiene cinco veces más capacidad que un DVD, y que serán liberados para el mercado de consumidor final en 2005. Así tenemos de todo: para pronto y para quién sabe cuándo.

MICROSOFT ABRIRÁ EL CÓDIGO FUENTE DE OFFICE

El omnipresente gigante de Redmond, presionado por el avance de Linux y otros programas gratuitos en la administración pública de diversas administraciones de todo el mundo, incluyendo desde ciudades hasta parises enteros, ha accedido a publicar el código fuente de su gama de productos Office en más de sesenta países. La empresa argumenta que, de esta manera, le resulta más fácil responder a las necesidades específicas de cada administración pública.

La apertura del código fuente se inscribe en el marco del Government Security Program (GSP, Programa de Seguridad Gubernamental) de la compañía de Bill Gates. Este programa, lanzado en enero de 2003, permite a los gobiernos tener acceso al código fuente de la gama de productos Microsoft Office (que incluye entre otros los programas Word, Excel y PowerPoint) aunque sin permitir su modificación.

Según Ted Schadler, un analista del instituto Forrester Research citado por el magazine norteamericano Wired, la apertura del código fuente de Office es una forma de luchar contra el ascenso de programas gratuitos como OpenOffice. Sin embargo, en la comunidad de usuarios de solftware libre predomina la opinión de que se trata de una medida populista, que ni siquiera se acerca a las ventajas del software abierto, pues no se puede modificar nada y el código fuente sólo queda al alcance de unos pocos.

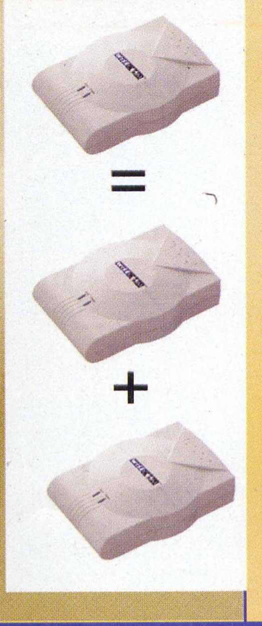
TELÉFONICA DUPLICA SU ADSL

A partir del 29 de setiembre de 2004 y hasta finales de noviembre Telefónica procede a duplicar la velocidad de sus lineas ADSL de sus 2,1 millones de conexiones de banda ancha.

Esta mejora no comportará ninguna subida de precio a los clientes. La migración no precisará de trámite alguno por parte de los abonados, y también será de aplicación a las nuevas altas de ADSL que se produzcan hasta que se complete el proceso, que no afectará al resto de prestaciones del servicio que el cliente tuviera contratadas, tales como cuentas de correo, antivirus y mantenimiento.

Así, las velocidades nominales de descarga de información serán el doble de las actuales, de forma que la modalidad básica de ADSL se situará en 512 kilobits por segundo (Kbps) para la bajada de información mientras que se conservarían los 128 Kbps de subida.

Para que los clientes puedan conocer en detalle las características de esta acción, se ha habilitado un web específico (www.telefonicaonline. com/masvelocidad), que cuenta con información al respecto, entre la que se encuentra la posibilidad de consultar el estado y las fechas previstas para el aumento de velocidad de su línea ADSL. También se detallan las mejoras aplicadas a cada plan de conexión.





NUEVA VARIANTE DEL VIRUS BAGLE

El martes 28 de septiembre, se detectó la aparición de una nueva variante del Bagle. El gusano, que se propaga por correo electrónico y redes P2P, ocasionó un elevado pico de infecciones a última hora de la tarde de ese día, lo que contrasta notoriamente con la poca actividad de virus y gusanos reportada en las últimas semanas.

Su principal vía de reproducción es a través del correo electrónico con un asunto como "Re:", "Re: Hello", "Re: Hi", "Re: Thank you!" o "Re: Thanks :)". Como texto solo se muestra el emoticón de una cara sonriente. El remitente es siempre falso, y no identifica al usuario que realmente lo envía.

La infección se produce cuando el usuario ejecuta el archivo adjunto, que puede llamarse "Price" o "Joke", y tener cualquiera de estas extensiones: .COM, .CPL, .EXE o .SCR

El gusano también se copia en las carpetas de conocidas aplicaciones P2P, para infectar a los usuarios que lo descarguen de allí al compartir sus archivos. Para ello se disfraza con múltiples nombres.

OPENOFFICE PUEDE CONVERTIRSE EN ESTÁNDAR

Aunque aún pendiente de confirmación, parece que la intención de la Comisión Europea pretende convertir el formato XML de OpenOffice en un estándar ISO.

El pasado mes de marzo la Comisión Europea se reunió con representantes de Microsoft y de Sun para analizar la adopción de un estándar para documentos ofimáticos. Ello hizo que Microsoft se apresurara a publicar las especificaciones del formato Word, facilitando de esta manera la compatibilidad a terceros.

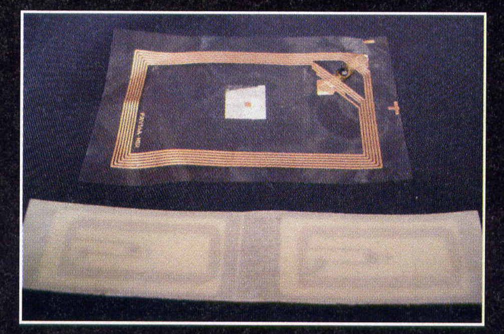
Finalmente, ello podría servirle de poco, ya que acudiendo al sentido común, la Comisión Europea parece haberse decantado por la alternativa libre, que presenta mayores niveles de transparencia, portabilidad a diferentes plataformas y accesibilidad.

Otro tanto a favor de OpenOffice.

Black Hat

En Las Vegas 28 y 29 de julio en uno de los más lujosos hoteles de la ciudad, el Caesars Palace, se ha realizado la quinta edición de Black Hat, la más famosa conferencia mundial sobre seguridad informática

En pleno verano, a 45 grados a la sombra, pero con una chaqueta gracias al generoso aire acondicionado de la instalación, más de 2000 personas han pagado caso 2000 dólares por cabeza para asistir a los nuevos ciclos de conferencias, que han alternado en cinco estrados a más de sesenta ponentes. Sí: Black Hat es un negocio multimillonario en el que los hackers de todo el mundo enseñan a una selección de IT de la industria y del gobierno las mejores estrategias para profanar sus sistemas de información.



← Dos distintas Smart Label. Con un coste de menos de 10 céntimos de euro la tecnología está a punto para invadir el mercado de la producción al por mayor. Los datos escritos en una etiqueta RF-ID pueden ser leídos por cualquiera.

En dos días, conseguir seguir todo el programa es imposible a menos que se tengan cuatro clones que puedan ir a las distintas conferencias que se producen en paralelo. en realidad la división por temas hace que cada uno encuentre siempre algo de su agrado y que así se vea en

2004

EL FUNDADOR

Jeff Moss, de 34 años, un físico delgado y longilíneo, fundador y organizador de Black Hat y de DefCon, explica que éste es sin duda el mejor año para Black Hat, un claro signo de que en el mundo de la informática finalmente el momento del relanzamiento ha llegado y las industrias vuelven a empezar a invertir. "Más de 2000 inscritos y un número de ponentes nunca visto, y todos altamente cualificados; hemos prestado mucha atención a su selección este año y los resultados están a la vista" confesó el día de la clausura, decididamente satisfecho por el éxito de la conferencia.

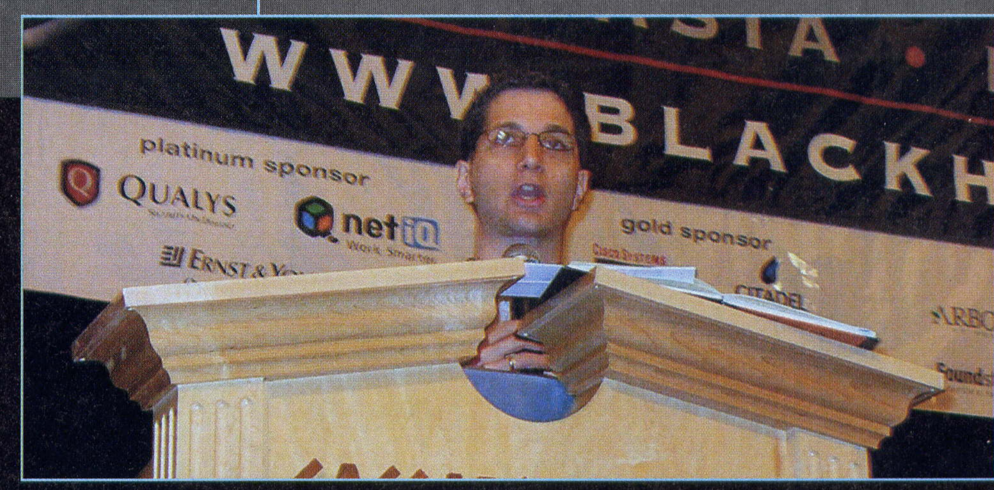
todo momento implicado en una conferencia, reduciendo al mínimo el tiempo perdido, pero en la práctica es bastante común encontrar dos conferencias que se dan a la vez y a las que se querría asistir. He aquí cuáles han sido los nuevos filones principales que han dado vida a Black Hat 2004:

- **Application Security.** Ya ha pasado la época de los cortafuegos, ¡ahora el vector principal de los ataques son las aplicaciones! Escribirlas correctamente desde el principio y sobre todo depurarlas teniendo presente la seguridad y la solución a este problema. En esta categoría las conferencias tratan sobre cómo verificar las aplicaciones contra los sitemas de ataque más comunes como SQL injection o buffer overflow, y cómo encontrar estas vulnerabilidades en las aplicaciones ya desplegadas.
- **Deep Knowledge.** Es la sección Hardcore de la conferencia. Aquí se tratan en detalle diversos argumentos; éste es el título de una conferencia: "¡No fiarse de nadie, ni de uno mismo, o el eslabón débil de la cadena podría ser precisamente el elemento que has escrito tú!"
- **Computer Forensics & Log Analysis.** Cómo descubrir y demostrar que alguien ha entrado dentro del propio sistema; IDS y estrategia avanzada como el HoneyNet o la baseline analisys se analizan y comparan para obtener los mejores resultados en este área.

Jeff Moss inaugura *la quinta edición de Black Hat. Con más de 2000 participantes, puede sentirse satisfecho*

- **Layer Ø.** También la capa de hardware tiene sus enemigos. Sistemas biométricos y los puntos fuertes y débiles de las medidas usadas normalmente para garantizar la seguridad de las instalaciones y el control de los accesos físicos a los locales de los servidores y las oficinas.
- **Policy, Management, and the Law.** No basta con tener una buena política, también es necesario que se respete y que sea útil y compatible con las leyes actuales.
- **Privacy & Anonymity.** En un país en el que la libertad de palabra garantizada por la primera enmienda se ve continuamente limitada y restringida en nombre de la seguridad nacional y de la lucha contra el terrorismo, cuáles son los métodos legales para recupe- ▹▹





← *Esta bolsa no anula los tag RF-ID que contiene la mercancía en su interior, sino que tiene una ulterior etiqueta RF-ID con un código especial que instruye al software para que ignore el contenido...*



evitar los ataques antes de que se efectúen.
Una correcta configuración permite interceptar el vector de ataque reduciendo al mínimo los falsos positivos; particular atención merece saber cómo las "regular expression" pueden ayudar en este campo.

Respecto al año pasado, aunque ha crecido la cantidad y la calidad de las conferencias, hemos notado una desagradable tendencia a omitir muchos detalles operativos en la presentación de las técnicas de exploit.

rar parte de la privacidad perdida y qué instrumentos se pueden utilizar para no perder más.
- Turbo Talks. Una nueva idea del 2004, con conferencias rápidas (unos 20 minutos) en las que se introducen argumentos rápidamente, lo justo para presentarlos y atraer la atención de la audiencia sobre ellos y poner las bases para un sucesivo análisis y estudio.
- Ø Day Attack. ¿Qué usan los crackers para atacar sistemas y cómo encuentran y dominan las vulnerabilidades? Existen intrumentos y métodos de aproximación para encontrar y utilizar los puntos débiles de los sistemas operativos y programas.
- Ø Day Defense. Así como hay métodos de ataque, hay sistemas Honeypot e IDS que se usan para descubrir y

Seguramente a causa del clima de tensión y de las querellas y sentencias fruto del DMCA sumado a la Patriot Act, los speakers se mantienen circunspectos, restando a la conferencia parte del valor que ha tenido los últimos años. Sin embargo, no han faltado la novedad y los detallados análisis que siempre caracterizan a Black Hat.

La llegada del RF-ID

Smart-Label y RF-ID son dos modos de indicar los nuevos sistemas de gestión de etiquetas, que mediante la electricidad producida por potentes campos electromagnéticos permiten a las etiquetas RF-ID activarse y transmitir y recibir datos de un punto informativo. En la práctica cualquier producto dentro de un negocio puede tracearse desde que entra en el punto de venta hasta que sale de la tienda en manos del cliente.
Así, el cliente que atraviesa la puerta de salida no tiene ni que detenerse a pagar: todo lo que contiene la cesta se puede inventariar y la puerta activa la tarjeta RF-ID enabled que el cliente posee, identificándolo y cobrando automáticamente de su cuenta. Parece muy interesante, si no fuera por un par de pequeños problemas de privacidad y de seguridad que introduce la tecnolo-

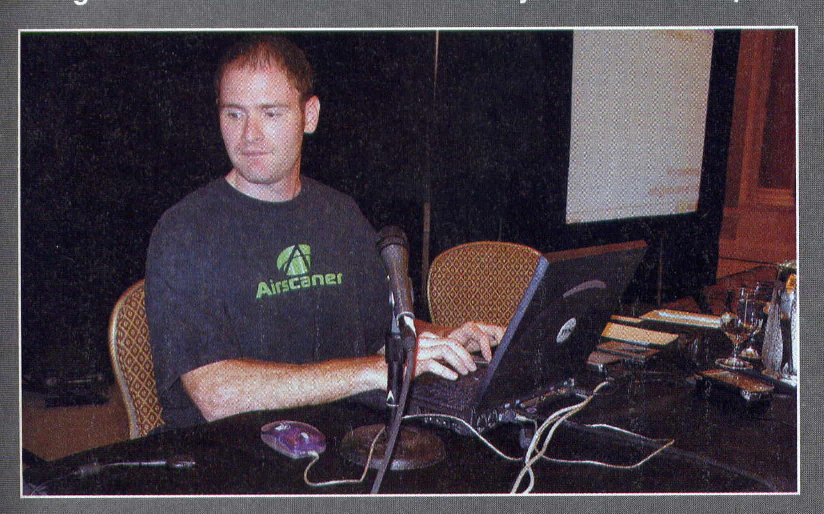
Esto es un lector RD-ID en versión compact Flash. Si alguien encontrara sospechoso pasear por un supermercado con un notebook en la mano, no se alarmaría ante un PDA y la lista de la compra. Pero... ¿y si va y se le ocurre cambiar las etiquetas?





← Un cambio de sesión o la hora de comer: la multitud de participantes de Black Hat.

gía. El esquema RF-ID permite leer y escribir cookies en las etiquetas o en la tarjeta, exactamente como en la navegación por Internet. Estas cookies pueden ser leídas por cualquier sistema RF-ID. Así, si tenemos la tarjeta del supermercado 1 y también la del 2, el supermercado 1 lo detectará y podrá incluso leer toda la información de la tarjeta del 2. En la práctica llevaremos encima nuestro perfil completo y todos, salvo nosotros, podrán leerlo. Es cierto que si todos tienen cautela en los datos que escriben en los TAG y en las cookies el problema sería mínimo, pero ¿quién lo garantiza? Además, los RF-ID no pueden desactivarse; una parte del código guardado dentro del chip no puede alterarse bajo ningún concepto (imagínate si el código del objeto se pudiera cambiar, la posibilidad de hacer un checkout automático con un televisor de plasma de 50 pulgadas como si fuera una tostadora...) por tanto el portal de salida se limita a borrar una parte de los datos pero el chip con el ID seguiría activo y legible para todos. Un escenario posible (pero improbable por la necesidad de usar una gran antena) sería que un ladrón escaneara la casa para verificar los electrodomésticos y otros bienes valiosos y decidiera dar o no el golpe: los RF-ID que tengamos en casa le dirán el modelo y la fecha de adquisición y si la garantía es válida o no... Y esto no es el futuro: Gilette y Benetton ya usan ampliamente RF-ID dentro de sus productos, y el mayor supermercado americano, Wall*Mart, con más de un millón de dependientes, prevé su uso en masa este mismo año. Es posible que ya estemos etiquetados sin ni siquiera saberlo. Es interesante notar, en aras de la privacidad, que es posible conectar al notebook o al PDA un lector y escritor de RF-ID por doscientos euros y que en los experimentos realizados los primeros bienes etiquetados han sido los fármacos con prescripción. Así, quien observe podrá saber hasta si nosotros o un familiar sufrimos algún tipo de enfermedad, ya que a pocos metros de distancia podrá leer las etiquetas de todos los fármacos que llevemos en el bolsillo o en la bolsa.
Es interesante notar que una bolsa especial para ocultar los RF-ID ha resultado ser un engaño, ya que simplemente consistía en un ulterior RF-ID que decía que no se leyera el contenido de la bolsa pero el contenido era legible; era leído pero el software debía gentilmente no mostrarlo en pantalla.



↑ *Seth Fogie, vicepresidente de la Airscanner presentó una conferencia sobre la simplicidad con que el malaware puede interactuar con nuestro PDA. Efectivamente, con la difusión de los pequeños ordenadores la situación será cada vez peor.*

Michael Raggo, un experto en criptografía de Verisign, ha mostrado en una conferencia la simplicidad con la que su programa en Visual Basic era capaz de encontrar la existencia de datos esteganográficos dentro de un archivo, insertados utilizando 13 aplicaciones distintas comerciales y freeware. Raggo ha demostrado así la inutilidad de estas aplicaciones, ya que el fin principal de la esteganografía es no dejar hallar la información y no tanto cifrarla.
Por añadidura, algunas aplicaciones para encontrar el contenido en fase de extracción lo marcaban con una firma, legible incluso mediante el Bloc de notas.

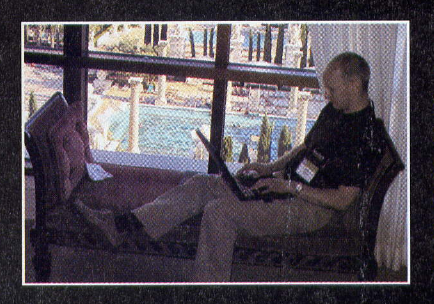
Un inglés y un alemán, Adam Laurie & Martin Herfurt, demostraron lo fácil que resulta tomar el control de un teléfono Bluetooth (BlueSnarfing) y, sin que lo sepa el usuario, realizar llamadas y transferir el contenido de la memoria, fotografías y agenda incluidos; al mismo tiempo, John Hering tomaba el control de un Nokia 6310i a una distancia de 1,7 kilómetros usando un fusil BlueSniper desarrollado por él y con un aspecto parecido al de un fusil de precisión, desde la ventana de su local en la planta once del Aladdin. Este argumento, no del todo nuevo, a decir verdad, es sin embargo tan importante que requiere un artículo dedicado a él en uno de los próximos números de la revista.

BlackHat 2004 ha terminado, las próximas citas son en Europa y Asia, los contenidos siguen siendo muy actualizados e interesantes y no puede faltar la invitación a visitar el sitio para descargar todas las presentaciones de los ponentes que estarán disponibles durante los próximos meses.

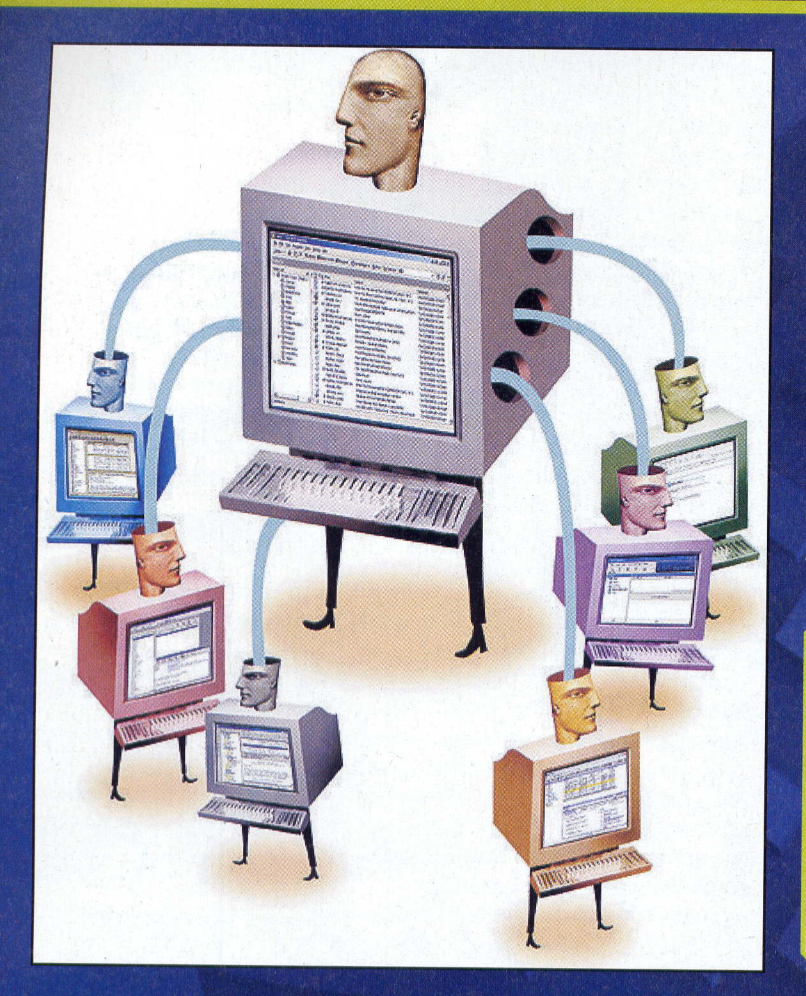
Silvio de Pecher

CONEXIONES

- www.vulnerabilite.com/dl/bh_2004/bh-us-04-
- www.blackhat.com
- http://www.vulnerabilite.com/dl/bh_2004/bh-us-04-geers.pdf
- http://www.airscanner.com/pubs/BlackHat2004.pdf
- http://www.stop-r_d.org
- http://www.boycottgillette.com
- http://www.boycottbenetton.com
- http://www.spychips.com
- http://www.thebunker.net/ release-bluestumbler.htm
- http://www.bluejackq.com/
- http://agentsmith.salzburgresearch.at/BlueSnarf/
- http://www.robosapienonline.com/



← *Las Vegas, unos 45 grados, en pleno desierto, una vista de las piscinas del Caesars Palace y un segundo de relax para un participante.*

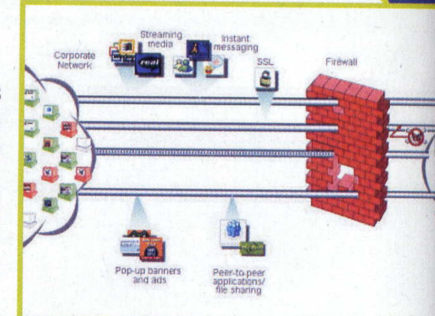


EL MEJOR

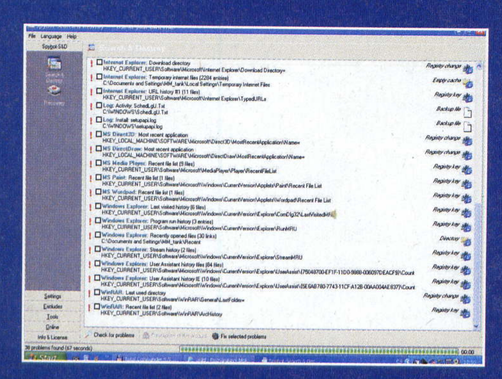
Hemos probado dos famosos programas gratuitos para eliminar programas no desados de Windows.

MALWARE

Contración de malicious software, software desarrollado para hacer daño a quien lo usa. Incluye virus, gusanos, troyanos e incluso el spyware, el software que captura información de un usuario sin permiso expreso de éste.



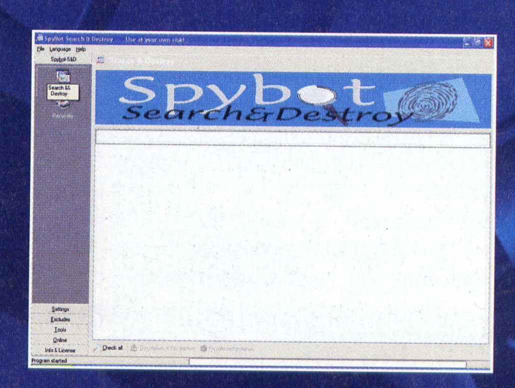
Un axioma de Windows es su facilidad para contagiarse con un virus u otro programa hostil y molesto, si no se es prudente y atento. ¿Pero es real el peligro? Lo hemos probado, y hemos hecho que un ordenador cumpla el papel de víctima. Lo hemos enviado por Internet a hacer cosas que no se deben hacer (como registrarse en los sitios porno -no por el sitio en sí, sino para ver qué hacen con nuestro correo- o bien descargar incautamente de sitios que prometen maravillas gratis y cosas así) y luego hemos puesto a prueba dos programas, Spybot y Ad-aware, ambos gratuitos. Como antivirus teníamos McAfee VirusScan Professional Edition y también la barra de Google para eliminar todo lo posible la publicidad indeseada. Por lo demás, todo hay que decirlo, cuando es necesario, ponemos trastear con el registro.



↑ *Estaría bien que fuera más radical en sus decisiones, pero Spybot trabaja bastante bien y encuentra lo que hay que encontrar.*

Por cantidad

Si nos guiamos por el número nadie supera a Ad-aware. Ha encontrado 47 archivos dudosos y entradas del registro equívocas cuando Spybot ha visto solamente cinco. En compensación, Spybot ha aislado todos los programas verdaderamente peligrosos, incluyendo uno que nos pensábamos que habíamos eliminado manualmente.

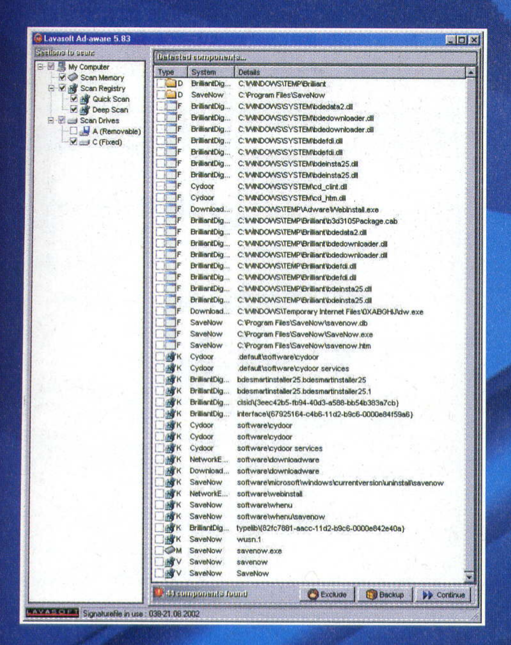


Una cosa que no nos ha gustado de Ad-aware es que su archivo de referencia estaba poco actualizado, con más de un mes de antigüedad. Esto no es positivo, porque los bancos de datos sobre el malware se actualizan continuamente y se requiere actualización constante, como con los virus. En cambio Spybot estaba al día, menos de una semana de antigüedad.

Por firmeza

Es importante ver qué medidas toman los programas antimalware contra las

ANTI-MALWARE



↑ Ad-aware localiza código no deseado en Kazaa. Una escena que se repite muy a menudo.

amenazas potenciales. Spybot ha aislado los problemas más graves y es el programa más prudente al sugerir si borrar un archivo o no. Sería mejor si se pudiera configurar que permite automáticamente el borrado, cosa que se puede hacer en fase de configuración. Ad-aware ofrece muchos más candidatos al borrado, pero también encunetra varios archivos que en realidad son más seguros.

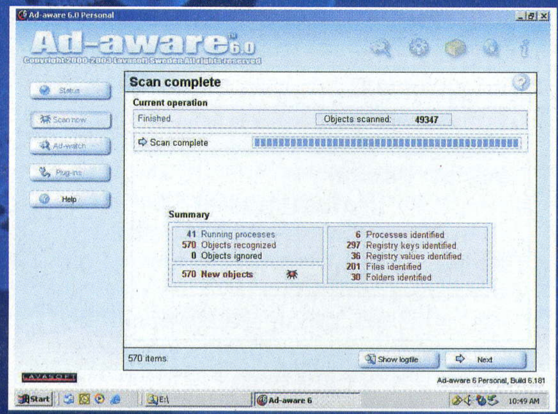
Los sistemas de ayuda son ambos válidos, si bien el de Spybot parece un poco menos actualizado. La última versión de los dos programas ofrece funciones de recuperación que permiten volver atrás si se dan problemas al eliminar un objeto. Naturalmente, si se usan las opciones avanzadas y se permite a tal o cual programa meter mano en el registro, es posible causar daños irreparables. Son opciones avanzadas con razón porque hay que saber lo que se hace. Spybot contiene un interesante opción de inmunización del navegador Opera e Internet Explorer, que activa funciones antimalware de estos programas normalmente inactivas.

Lo que no nos gusta

Poca cosa. Spybot ofrece una opción de copia de seguridad del registro de Windows, pero cuando la hemos probado no ha funcionado. Ad-aware se comporta bien, aparte de crear un icono en el escritorio y una entrada en el menú Inicio sin que se lo hayamos solicitado.

Conclusiones

Nuestro veredicto es: empate. Spybot captura los peligros principales con uno o dos clics del mouse; Ad-aware requiere quizás algo más de atención, pero ejecuta una limpieza más profunda. Ocupan poco espacio en disco, se actualizan a menudo por Internet y son gratuitos. Por lo que valen, creemos que lo mejor es tenerlos ambos, trabajando en equipo.



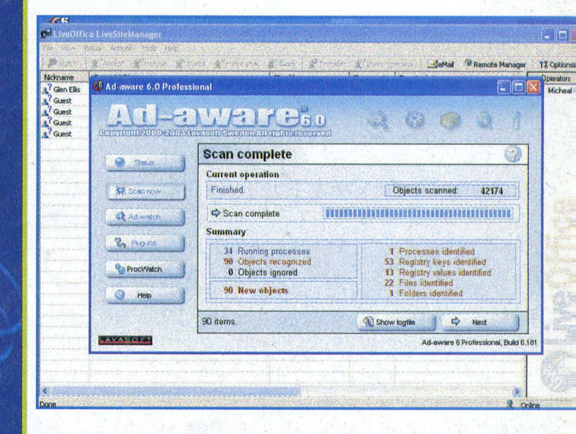
↑ Lo bueno de estos programas es su precisión al indicar lo que han encontrado en el ordenador.

AD-AWARE 6 PERSONAL

Bueno: Caza un número increible de amenazas de malware y, de serie, permite decidir cómo comportarse para cada una.

Malo: Podría ser más agresivo al identificar los archivos a borrar, tiene actualizaciones poco frecuentes y pone iconos y comandos en el escritorio y el menú Inicio sin preguntar.

Dónde: gratis para uso personal en http://www.lavasoftusa.com.

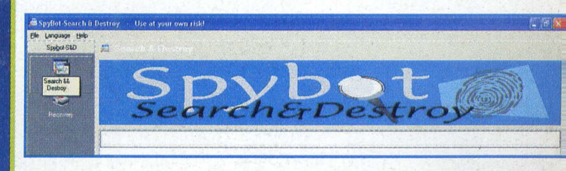


SPYBOT - SEARCH & DESTROY 1.3

Bueno: aisla y resuelve los peores peligros para el principiante y ofrece buenas opciones avanzadas para los más lanzados.

Malo: La ayuda no está muy actualizada y, con la configuración predeterminada, tiende excesivamente a conservar los archivos dudosos.

Dónde: gratis en http://www.safer-networking.org.



SOLSTICIO

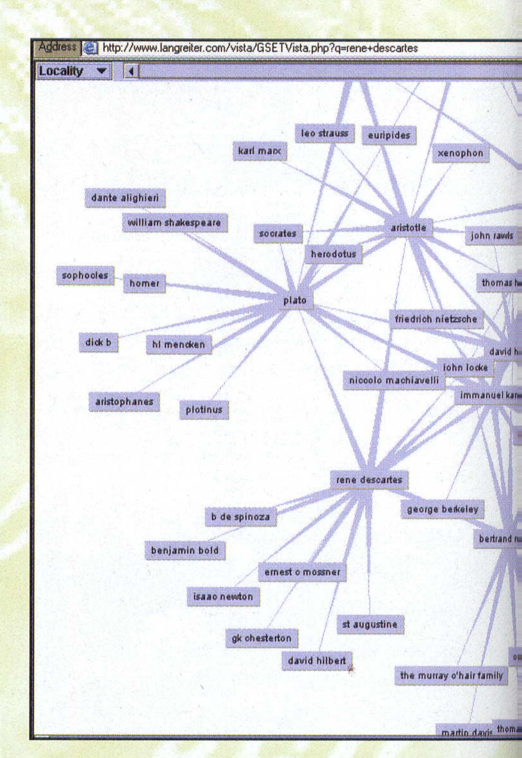
Retrato de qué es (y no es) un HACKER desde el punto de vista técnico y moral



↑ De Sócrates a Leonardo da Vinci, y podríamos seguir hasta... ¡Hacker Journal!

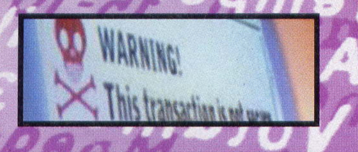
Session Start:
Sat Dec 21 03:54:06 2003
Session Ident: Rotten

<wisdom> Hola.
<rotten> Hola.
<wisdom> No entiendo el significado del término hacker.
<rotten> Un hacker es una persona experta y entusiasta de algo. Hay hackers de música, de matemáticas...
<wisdom> Pero entonces, ¿por qué las revistas de hackers hablan sobre todo de informática?
<rotten> El término se utiliza habitualmente en informática.
<wisdom> ¿Entonces un hacker es una persona experta y entusiasta de la informática?
<rotten> ¡Exacto! Pero tiene conocimientos superiores a los del usuario medio.
<wisdom> ¿Y en qué consisten?
<rotten> El hacker sabe programar bien y rápidamente especialmente en lenguajes como C y Perl.
<wisdom> ¿Pero ésta no es la definición de un programador?
<rotten> Un hacker es un programador, pero su capacidad va más allá.
<wisdom> ¿Y hasta dónde llega?
<rotten> Los hackers son los mayores expertos en informática.
<wisdom> Entonces, ¿quien más sabe de ordenadores tiene que ser un hacker?
<rotten> ¡Naturalmente!
<wisdom> ¿Entre sus capacidades se encuentra obtener el control de un servidor remoto?
<rotten> No, quien realiza acciones de este tipo se denomina cracker.
<wisdom> ¿Pero existe alguien que sepa más que un hacker de ordenadores? Si el cracker sabe hacer más cosas que un hacker, es quien más sabe sobre la red.

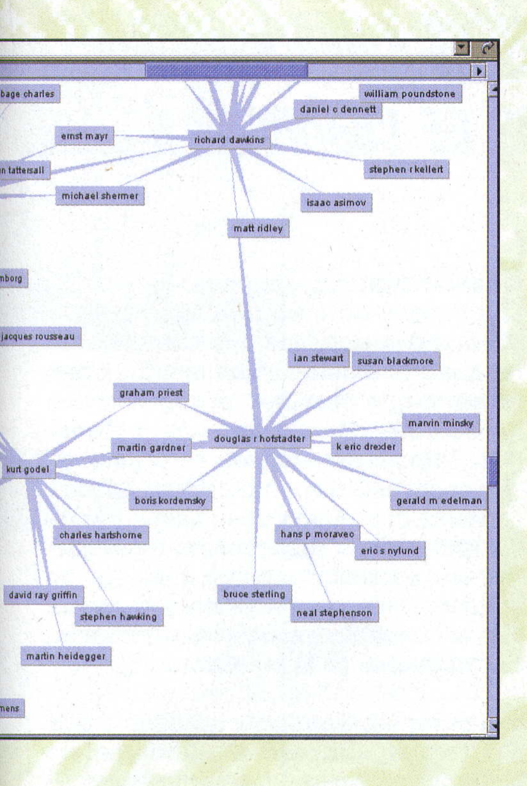


<rotten> No, el hacker también puede hacerlo, pero esto no quiere decir que lo haga.
<wisdom> Pero entonces, ¿cómo puede un hacker dominar este arte? Sabe lo mismo que un cracker, pero ¿cómo lo ha aprendido? ¿De la teoría? ¿Ha comprado libros de hackers y los ha estudiado?
<rotten> ¡Sin duda!
<wisdom> Pero ¿existen libros así, que lo explican todo sobre cómo convertirse en hacker?
<rotten> No, pero en Internet se encuentra el funcionamiento de prácticamente cualquier cosa.
<wisdom> ¿Pero cómo puede un hacker conocer este arte sólo leyendo manuales en la red? Tiene que haberlo probado.
<rotten> No, leyendo manuales y documentación ya no es necesario probarlo.





de invierno

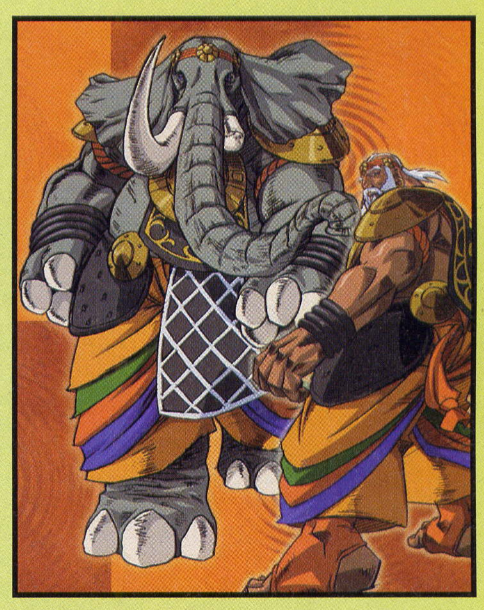


<wisdom> Entonces estudia sólo la teoría.
<rotten> Exactamente.
<wisdom> ¿Y cómo puede ser el conocimiento teórico del hacker más grande que el mismo conocimiento teórico del cracker, que encima tiene conocimientos prácticos? A menos que el hacker también los posea.
<rotten> Correcto.
<wisdom> ¿Y cómo puede tenerlos, sin haberlo probado nunca?
<rotten> Probando en equipos propios, sin bajar al nivel del cracker, que ataca equipos de otros.
<wisdom> Así que un hacker debería contar con una red propia con equipos diversos.
<rotten> Sí.
<wisdom> No creo que muchos puedan permitirse un gasto de esta magnitud.
<rotten> Basta con dos equipos, uno que prepara el ataque y otro que lo recibe.
<wisdom> Pero podría probar con uno o máximo dos sistemas operativos. ¿Cómo puede convertirse en experto en todos los demás? Tendría que tener una decena de discos duros, o bien dos discos duros grandes con particiones. En cualquier caso es un gasto. Así que ¿una persona no puede llegar a ser hacker a menos que sea rica?
<rotten> Desde luego que sí...
<wisdom> Y para poder probar un simple ataque man-in-the-middle debería tener al menos tres equipos. Pero ¿cómo conseguir activar un firewall sin tener un cuarto equipo conectado a Internet y por lo tanto un quinto fuera de la red?
<rotten> Pero actuando así un hacker adquiere más conocimientos de un cracker, repetando plenamente la legislación.
<wisdom> Hay cosas que no se encuentran e los libros o en la propia red. Comprender por qué te han atacado, dónde te has equivocado, cómo mejorar, nociones obtenidas por la experiencia y que comportan riesgo.
Por ello, el hacker sabe menos que un cracker y por lo tanto es inferior técnicamente, o bien el hacker es una persona que tiene por costumbre superar sus límites intentando obtener el control de servidores remotos cada vez más protegidos. Esto es ilegal; sin embargo, así como existen hackers devastadores, hay otros que advierten a los administradores sobre los fallos en sus servidores.
Distingámolos por su moralidad, no por el simple hecho de ser hacker.

Session Close:
Sat Dec 21 04:22:31 2003

Diálogo socrático

Esto es un diálogo socrático: rotten se cree docto y explica lo que sabe y cree que es correcto; wisdom corresponde a Sócrates quien, fingiéndose un falso ignorante, hace hablar a rotten y demuestra por el absurdo que sus tesis son erróneas.
Demostrar por el absurdo significa secundar las opiniones de una persona y dejar que ésta cree un paraíso; de este modo las tesis que se creía que eran ciertas se revelan como falsas. Rotten pronuncia frases inspiradas en la Jargon File y otras que se leen en IRC, y lo que dice Wisdom es nuestro punto de vista.





¿Libertad de XOR?

Ès interesante preguntarse si el copyright sigue vigente después, o a pesar de, una transformación matemática de contenido digital

Supongamos que tenemos dos archivos binarios protegidos por copyright y los unimos bit a bit como argumentos de una función lógica XOR. Obtenemos un tercer archivo que no contiene ningún dato efectivamente presente en uno u otro archivo. ¿Este archivo está protegido por copyright? Y si es así, ¿quién tiene el derecho de copia?

El tercer archivo ciertamente no es una copia directa de los originales; su contenido es realmente distinto. Tampoco es una derivación de los dos archivos anteriores, puesto que no contiene ninguna parte reconocible.
Pero se mantiene el hecho de que, al llamar otra función XOR con como argumentos el tercer archivo y uno de los dos originales, se obtiene de inmediato el otro original. Es sabido que el tema del copyright, aplicado al mundo digital, crea graves problemas, y esta es una de tantas demandas posibles que complicarán el cuadro. Existen instrumentos open source que permiten profundizar en tales consideraciones, como Monolith (http://monolith. sourceforge.net/). Monolith está disponible para cualquier sistema operativo y esencialmente calcula el XOR de dos archivos como queramos, escribiendo como resultado un tercer archivo con la extensión .mono. Es el concepto expuesto anteriormente, traducido en la práctica.



Dos archivos protegidos por copyright los fundimos en uno. ¿El nuevo archivo también está bajo copyright?

La discusión bascula entorno a dos extremos. Uno de ellos sostiene a ultranza el copyright: a partir del archivo original, lo que se obtenga luego es siempre, de uno u otro modo, un derivado. En el otro extremo se sitúan quienes sostienen que, al ser el archivo original y el archivo con el XOR totalmente diferentes, cuesta ver cómo uno de ellos pueda transmitir el

MONOLITH

↑ Monolith, programa a base de XOR para experimentar los temas estudiados en estas dos páginas, se puede descargar para cualquier sistema operativo en http:// monolith.sourceforge.net.

//Cubierta original de la "The hunting of the snark" de Lewis Carroll

Poema en versículos Libre de copyright

XOR, EL GRAN MEZCLADOR

Como otras funciones lógicas, XOR también acepta dos bits de entrada y devuelve un tercer bit de salida en función de cómo eran los dos bits originales. El esquema de su funcionamiento es el siguiente:

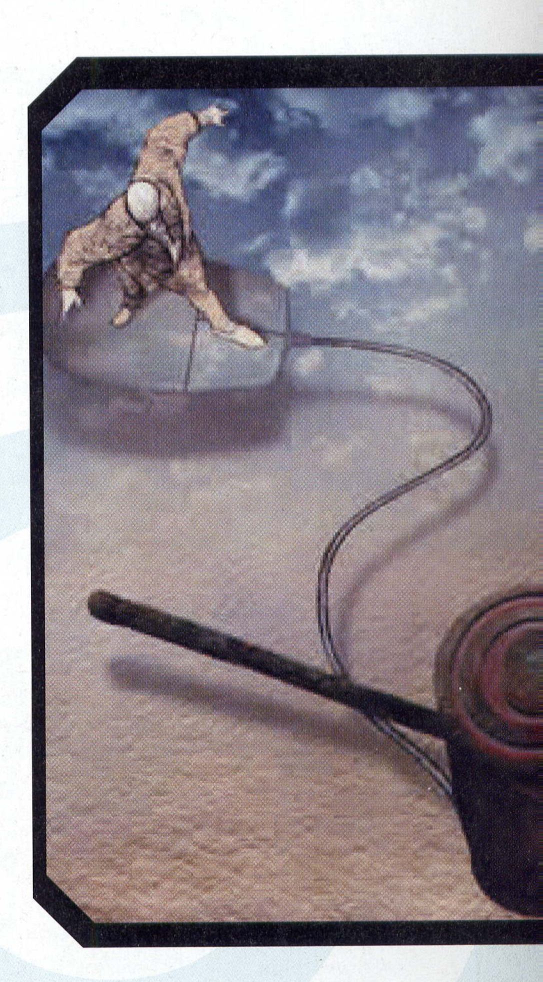
BIT INPUT 1	BIT INPUT 2	RESULTADO
0	0	0
0	1	1
1	0	1
1	1	0



derecho de copia al otro. Si escuchamos una canción por la radio, la silbamos, llegamos a casa, la tocamos con la guitarra y grabamos nuestra ejecución, ¿cuándo se ha producido la violación del copyright?

Recientemente se razonado sobre el discurso y se ha empezado a poner en marcha un sistema alternativo y poco eficiente, pero ingenioso, de distribución segura de archivos. La idea es crear depósitos de archivos de 128 KB llamados pad. Cada pad en sí no contiene absolutamente nada inteligible, pero si por casualidad se combinan varios pad juntos mediante XOR, resulta que de pronto dentro de los pad aparece información. Ningún pad contiene toda la información correspondiente, que está distribuida de modo arbitrario dentro de los pads. Lo interesante no es tanto que un archivo pueda ocultarse o confundirse, sino que en determinado momento las personas pueden trasmitir o conservar pads sin saber en absoluto qué hay en su interior.

El cerebro se parece mucho a un codificador de MP3: es relativamente eficiente, pierde por el camino algo de la señal y si uno se concentra consigue mantener un bitrate elevado.



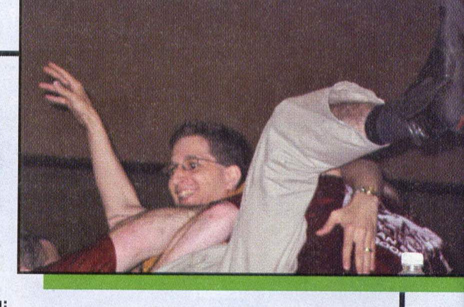
Algún usuario más astuto – o más atento a estos problemas – irá más allá y, mediante XOR, creará pads visiblemente inocentes. Algo que, con el XOR adecuado, genere una copia de una obra de Lewis Carroll, o un grabado de la Divina Comedia de Doré... algo que esté completamente libre de copyright. O información libre, como una serie de decimales del famoso número pi (3,14159), o en su lugar de una serie de Fibonacci (1, 1, 2, 3, 5, 8, 13, 21, 34...). Interrogado eventualmente durante un juicio sobre los pads en su poder, mostrará que conllevan información absolutamente inocua, que no está prohibido divulgar, ni pasar por un XOR.
El tema es controvertido, Lo importante es no hacer nada ilegal... y saber lo que se hace.

DefCon

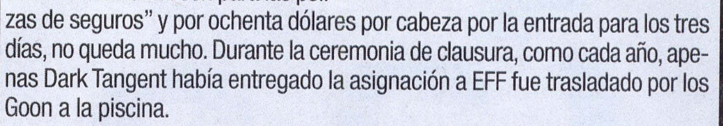


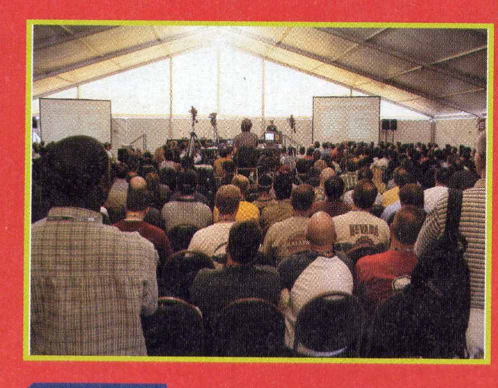
Las Vegas 30/7 - 1/8: cinco mil hackers convocados, un gran evento, seguramente el que tiene una historia más larga, probablemente el que tiene un mayor número de participantes, tal vez el más importante

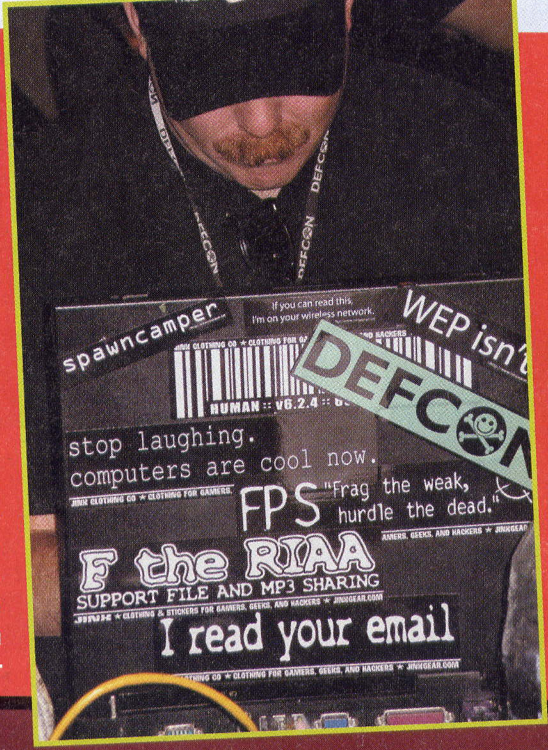
>> JEFF MOSS

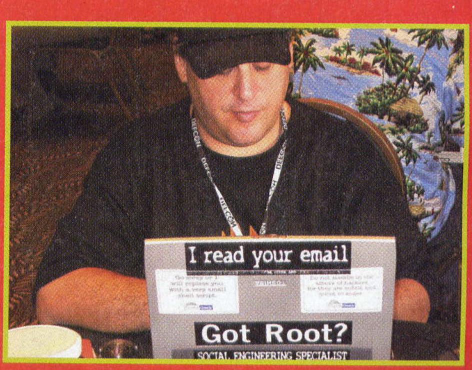


Cuidado con confundirlo con DefCon, Dark Tangent, ahora con treinta y cuatro, es el fundador de la manifestación: "En el 92 cuando habíamos empezado queríamos pasar el testigo de las BBS a Internet y éramos poco más de una cincuentena, y ahora somos cinco mil" dice, no sin una pizca de justificado orgullo por su criatura. Mientras que Black Hat es la gallina de los huevos de oro (¡un accidente si sus huevos son de oro!) DefCon es y sigue siendo una gran fiesta caótica, donde miles de hackers se reúnen y pasan juntos tres días, en una gran kermesse. "Ha sido un error", dice Jeff respondiendo a nuestra petición sobre el origen de su nombre, "cuando era joven durante una mudanza se perdió misteriosamente la caja con mis cómics y entre ellos había uno que me gustaba especialmente, D'Arc Tangent, como la función matemática, y tomé ese nombre por error, ya que había perdido el cómic… Actualmente estoy convencido de que la desaparición de la caja fue cualquier cosa menos casual, y que mis padres tuvieron mucho que ver". Dark Tangent ha devuelto parte de lo recaudado de las manifestaciones a la EFF (unos 3.600 dólares). "El alquiler del albergue nos cuesta doscientos cincuenta mil dólares, y otros ciento ochenta mil son para las pólizas de seguros" y por ochenta dólares por cabeza por la entrada para los tres días, no queda mucho. Durante la ceremonia de clausura, como cada año, apenas Dark Tangent había entregado la asignación a EFF fue trasladado por los Goon a la piscina.









Este año la afluencia fue sin duda excesiva para la estructura del Alexander Park y muchos hicieron cola durante mucho tiempo, la temperatura era de 45 grados a la sombra (ah, si se podía encontrar una sombra…) para conseguir acceder a la conferencia deseada. Quizás en este punto para el año que viene alguien debería hacer algo… Como en años anteriores se ha tratado de una gran fiesta en la que los tres ciclos de conferencias con sus casi cien ponentes no fueron el centro de interés, sino un

SCAVENGER HUNT

La caza del tesoro (scavenger hunt) es una constante fuente de diversión para todos. Es sugestivo ver los objetos más extraños o personajes con cazadoras claveteadas y cortes de pelo imaginativos que se movían por los salones esperando (?!?) pasar inadvertidos.
La caza del tesoro consiste en una larga lista de objetos que hay que encontrar o de acciones a cumplir y documentar, y cada objeto de la lista tiene su valor en puntos. Al final de la caza quien tiene más puntos gana. He aquí un extracto de la lista de este año:

Objetos
Billetes extranjeros (20 puntos)
Gemelos idénticos, vivos (50)
Paquete de helado de los astronautas (lo venden en Cabo Cañaveral) (75)
Un billete de dos dólares (25)
Un libro firmado por William Gibson (75)
Foto de uno del team con un guardacosta de Las Vegas en uniforme (100)
Mapa de la Tierra media (20)

Acciones
Baile en la piscina (100 si bien hecho)
Todos vestidos de drag queen (65)
Hacer una larga pajita y beberse una lata del techo (100)
Hacer dar la extremaunción por parte de un sacerdote a uno del team (60)
Pedir a un Goon: "¡enséñame a hackear!" (15)
Pintarse la cara como un payaso (25)
Comer una loncha de pizza en 10 segundos (30 si sobrevive)
Poner a uno del team en una maleta (25)

Éste es el sitio oficial; en los próximos días se publicarán las fotos más interesantes de los participantes. http://www.scavengerhunt.org/

CANNONBALL RUN

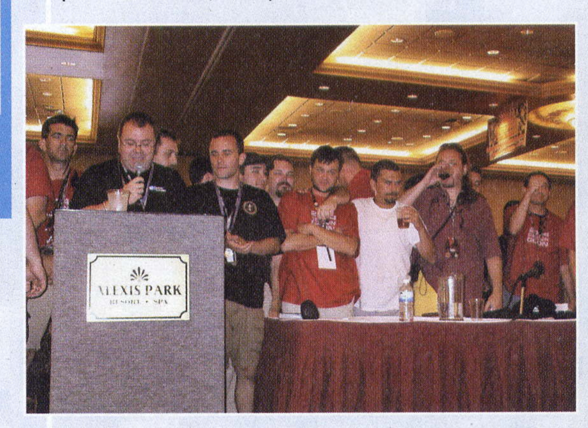


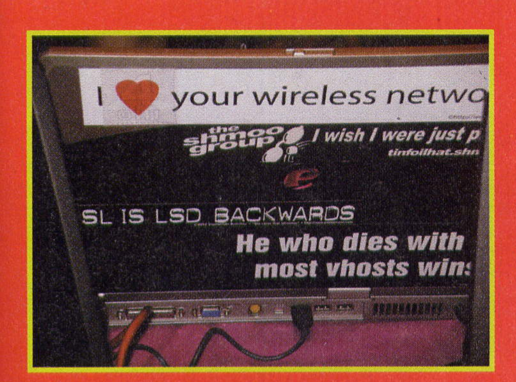
Por tercer año consecutivo se ha llevado a cabo la Cannonball, una carrera que va de Redondo Beach (en California) al Alexis Park Hotel. Obviamente se desaconseja por parte de los organizadores superar los límites de velocidad, entre las cincuenta y las sesenta y cinco millas por hora, pero algunos competidores parecieron tomarse este consejo a la ligera, recorriendo las trescientas millas de distancia en menos de tres horas, con una media de unas ciento diez millas por hora: ¡menudos cohetes! Este año estaba en la salida la TV y justo después llegó también la policía. Tras la salida el policía se marchó diciendo: "Disculpadme, pero tengo verdaderos crímenes que perseguir". Foto y crónica en el sitio http://moloch.org/cannonball/

LOS GOON

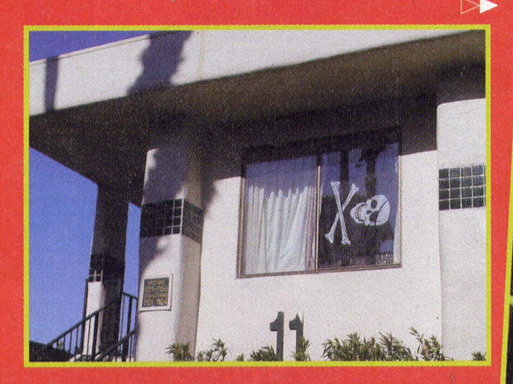


Los Goon son la policía de la manifestación. Irreductibles e imperturbables a las provocaciones y a otros insultos, administran la justicia para regular el acceso a las salas, y no han tenido la vida fácil para los malhumores (escasos) de la gente por la falta de espacios y las largas colas al sol. Litigar con un Goon es tan útil como hacerlo con un poste eléctrico, elemento con el que el Goon comparte la dureza, la impavidez e incluso la inteligencia. De aquí proviene la pregunta: "¿has discutido alguna vez con un Goon?" ¡Desde luego! Los Goon tienen su propio sitio: http://www.goons.org/
http://www.defcon.org/html/links/dc-goons.html





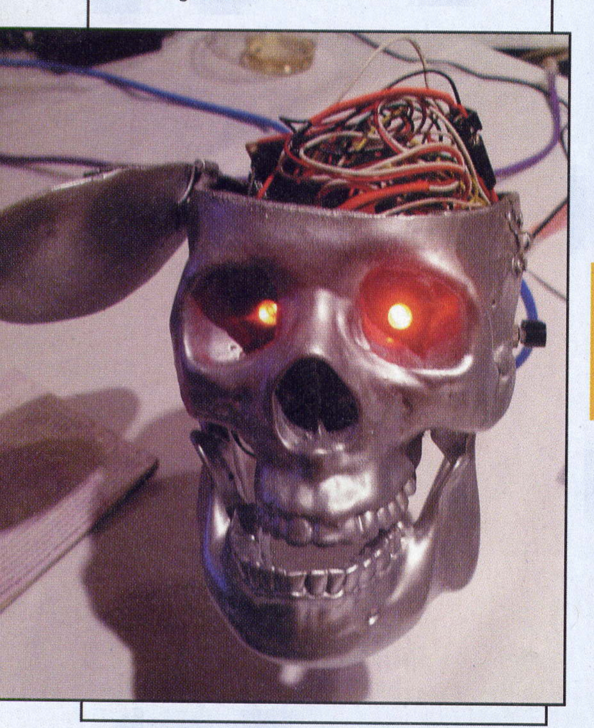
agradable fondo. Aquí se viene para encontrarse, discutir o para conectarse a redes wireless en busca de datos interesantes. Pero los mejores momentos de la convención se encuentran en un momento crítico: entre DMCA (Digital Millennium Copyright Act) y la Patriotic Act la vida del hacker no es ahora nada fácil. En EE.UU existe la primera enmienda, es decir, el derecho absoluto a la libertad de expresión y de palabra. Esto querría decir que puedo escribir cualquier cosa, desde pornografía hasta mensajes políticos, pasando por todos los tecnicismos necesarios para construir





>> IP APPLIANCE

Por primer año se ha intentado hackear una tostadora. Un appliance (electrodoméstico) que haga algo más que aquello para lo que ha sido construido. El concurso no ha tenido un gran éxito y su único competidor ha vencido con un cráneo gobernado desde un notebook capaz de abrir y cerrar los ojos, abrir y cerrar la boca y usar un sintetizador de voz. Pero es un principio, y para el año que viene ya se han comprometido más competidores en la segunda convocatoria.



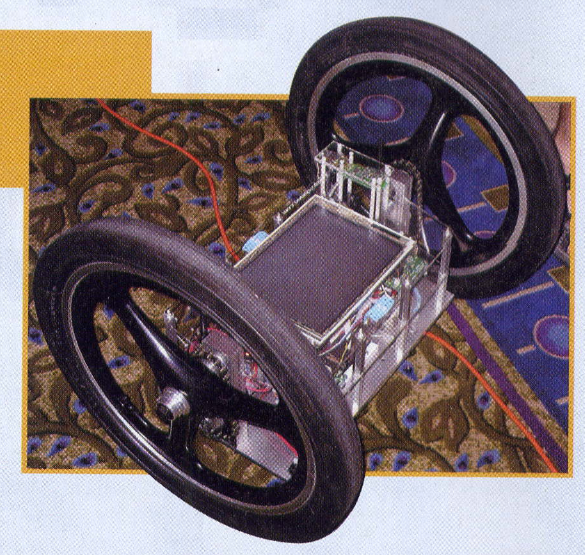
>> ROOT FU

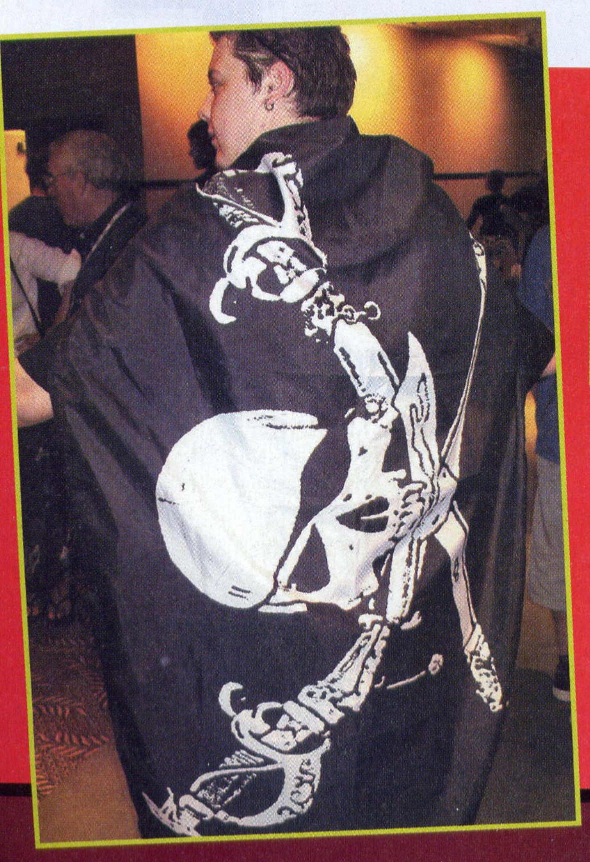


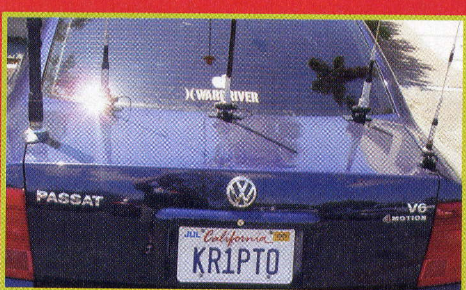
El arte de hackerar sistemas... Este año ocho equipos se enfrentaban en nueva plataforma: controlar y administrar diversos sistemas ganando puntos con accesos dentro de los demás sistemas (ataque) y no perdiéndolos evitando los accesos de otros al propio sistema (defensa). La batalla por primera vez ha durado 36 horas seguidas y los diagramas de los ataques han mostrado diferentes reacciones a la cafeína del equipo. Se ha visto qué importante es el ataque, pero también la defensa porque el equipo que ha dominado la competición consiguiendo atacar a todos los demás competidores finalmente la perdió ya que no consiguió guardar en casa todos los puntos tan fatigosamente conquistados...

>> ROBOT WAREZ

Otro concurso con pocos competidores, ganado por este robot que ha llevado las palas de ping pong de un contenedor a otro en un tiempo récord (primera edición, único participante, ¡ha sido un récord sin duda!). Sin embargo este concurso ha despertado un gran interés por parte del público y muchos han decidido participar el año que viene. El otro robot era capaz de encontrar conexiones WiFi, desplazarse hacia su origen y mostrar en la pantalla el password utilizado.







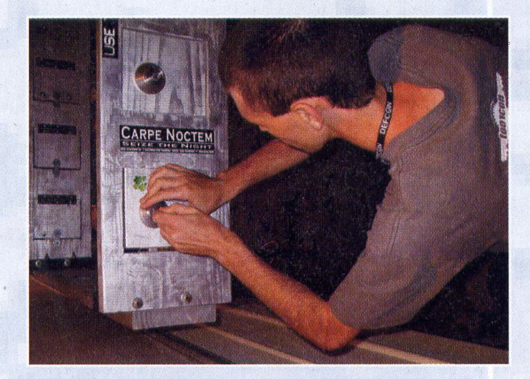
una dirt bomb o escribir un programa capaz de aprovechar una vulnerabilidad conocida de un software o de un sistema operativo. Esto era cierto hasta hace algún tiempo. La "guerra al terrorismo" y el DMCA se han utilizado metódicamente para combatir la búsqueda de los hackers por el software y ahora hay cientos procesados o en la cárcel y miles que han sido llamados a juicio. En los EE.UU de hecho los tribunales funcionan y en un par de meses te puedes encontrar ante el juez, y esto es algo positivo, pero una causa civil puede durar fácilmente cinco o diez años siendo generosos, por lo que el problema principal es que un avogado en EE.UU cobra al menos doscientos dólares a la hora. El coste del avogado puede superar fácilmente los veinte mil dólares (cien horas de trabajo). Por ello, para combatir la insidia de la libertad de palabra se usa continuamente la sombra de la citación porque si se publica algo en base a la primera enmienda (¡legítimo!) puede llegar una citación por sospecha de violación del DMCA por haber hecho "reverse engineering" o haber metido las narices en una ruti-



» LOCKPICK

Se está poniendo de moda en Europa, procedente de EE.UU, el arte de abrir cerrojos, un deporte nacional entre los hackers americanos. Recordando una antigua tradición del MIT, cuando los ordenadores se cerraban con llave de noche, dejando toda aquella potencia computacional inutilizada y el arte de abrir las puertas se convirtió en una virtud "indispensable". Dos son las competiciones más apreciadas: la competición por tiempo en un solo cerrojo y la competición en salida, donde gana quien consigue abrir el mayor número de cerrojos de dificultad creciente. Los cronómetros se detuvieron en el tiempo récord de 7 segundos para el primer caso. Sorprende el resultado de la competición de salida: de ocho cerrojos previstos, el segundo y el tercer clasificado no pasaron del segundo cerrojo, y el ganador se quedó en el séptimo por falta de tiempo, pero probablemente habría abierto el octavo. En nuestro país resulta difícil comprender, entender y tolerar este deporte, ya que la sola tenencia de las herramientas es ilegal, pero es un verdadero espectáculo ver a estos artistas trabajando en lo suyo.







» WARDRIVE

Por primera vez este año el wardrive ha evolucionado en 4 distintas competiciones. La primera fue el clásico wardrive, pero sin límite de tiempo, y se clasificaron en primer y segundo lugar dos participantes que se movieron durante treinta horas ininterrumpidamente, con número de accesos encontrados enormemente superior a los de los demás participantes. Tag me, consiste en encontrar un AP con SSID: TAGME que se conecta cada diez minutos y tiene un web server Windows 2000, entrar en el sistema y escribir un archivo de texto. Encontrar el punto de acceso fue fácil, pero ningún participante consiguió entrar en el sistema ¡a pesar de que dos passwords eran iguales a los nombres de los usuarios! Running Man es una caza del hombre; el hombre, en este caso una mujer, cuenta con un AP de baja potencia y un web server con información que hay que encontrar y verificar con la correspondiente firma PGP. Fox and Hound es un nuevo formato en el que es preciso descubrir un punto de acceso que funciona durante quince segundos por minuto. La dificultad principal para los competidores fue puramente ambiental: ¡pocos minutos después del inicio de la competición había decenas de access point con el mismo SID buscado y con la misma mac address! Por otra parte, si se quieren hacer las cosas fáciles, ¿por qué ir hasta el DefCon?

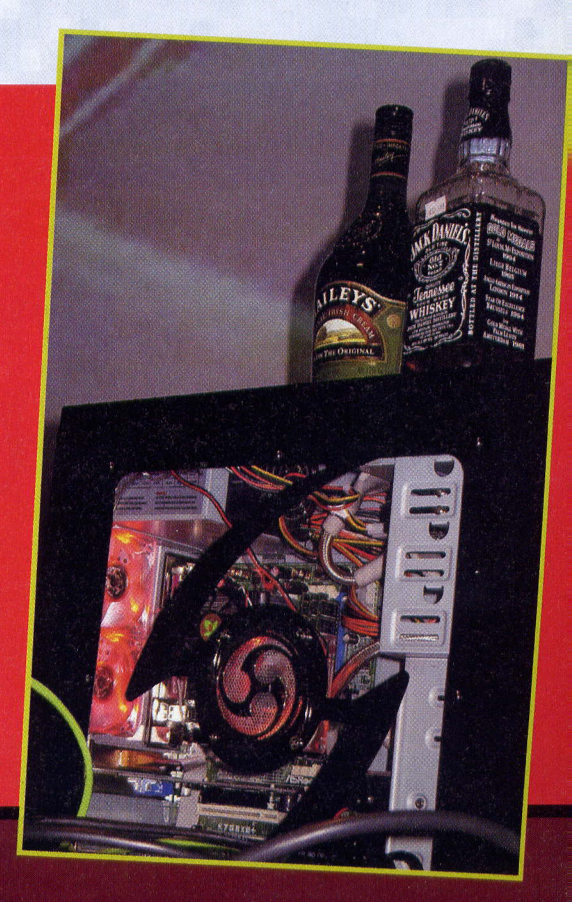




na cifrada. Aunque no sea cierto hay que poner sobre la mesa los veinte mil dólares necesarios para pagar al abogado y... ¡adiós primera enmienda! Por ello este año se han visto muchas bocas cerradas que no han entrado en detalles por miedo a una denuncia. Sin embargo, las conferencias han sido interesantes y podéis leer los contenidos en el sitio de DefCon, donde se publicarán durante los próximos meses (http://www.defcon .org/). Paralelamente a las conferencias se desplegaron una serie de eventos oficiales o no, que han atraído el interés de los participantes. Algunos eventos son nuevos, otros tienen una historia a sus espaldas que se pierde en las primeras ediciones de la manifestación.

Silvio de Pecher





ARCHIVOS INVISIBLES DE WINDOWS

Dónde están, qué hacen, por qué son invisibles y, sobre todo, ¡cómo llegar hasta ellos!

Hemos hablado ya de los archivos index.dat que Microsoft oculta en Windows para que no sean vistos si no es desde DOS. Contienen nuestro historial de navegación y otros datos que Microsoft, por cierto, no quiere que veamos. Los archivos index.dat se encuentran en

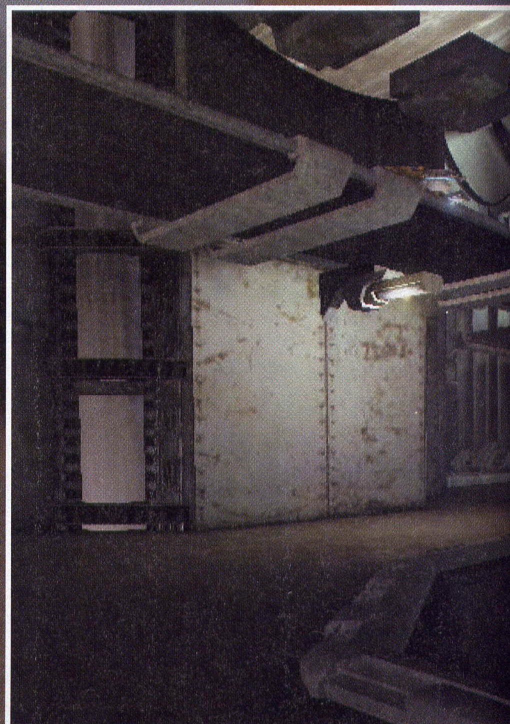
```
c:\windows\history\history.ie5\index.dat
c:\windows\tempor~1\content.ie5\index.dat
```

El algunos casos los archivos pueden tener el nombre alternativo de mm256.dat y mm2048.dat, y estar en

```
c:\windows\tempor~1\
c:\windows\history\
```

O bien también en

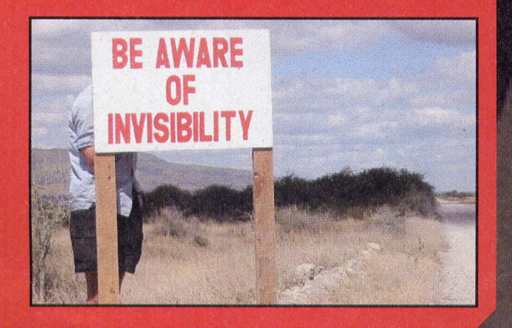
```
c:\windows\profiles\%usuario%\...
c:\windows\application data\...
c:\windows\local settings\...
c:\windows\temp\...
c:\temp\...
```



En los meandros de nuestro sistema se ocultan archivos invisibles que Microsoft quiere mantener así...

EN EL REGISTRO

Según Microsoft el Registro del sistema es un archivo central que contiene únicamente datos sobre la configuración de Windows y de los programas. Bobadas. Para empezar, contiene también información sobre los últimos URL que hemos escrito en Internet Explorer, en concreto los que el navegador recuerda para el autocompletado automático. Afortunadamente, se pueden borrar. Abrimos el Registro del sistema mediante Inicio -> Ejecutar -> regedit. Las claves del registro que nos interesan están en HKEY_USERS/Default/Software/Microsoft/Internet Explorer/TypedURLs/ y HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs/.



Depende de como esté configurado el PC y, por ejemplo, qué hay en el archivo autoexec.bat.
Paseando por el sistema es posible hallar algún otro archivo index.dat, aparentemente menos importante para nuestra privacidad.
Quien quiera puede dedicarse a localizarlos en su sistema.

Borrar por seguridad

No es difícil borrar los archivos .dat, una vez sabemos que existen. Atención: borrarlos significa destruir archivos de caché, temporales, de historial, etc. Podemos hacerlo si lo deseamos, pero sólo si sabemos qué significa: no lo hagamos simplemente por probar.

Reiniciamos el equipo y, mientras arranca, pulsamos la tecla F8 y entramos en la modalidad a prueba de fallos con línea de comandos.
Al hacer esto podemos trabajar desde DOS y escribir comandos que de otro modo no conseguiríamos que funcionaran. Los equipos con el antiguo Windows ME requieren un boot desde un disquete para entrar en modalidad de línea de comandos.

```
C:\WINDOWS\SMARTDRV (carga smartdrive para acelerar las cosas)
CD\
DELTREE/Y TEMP (borra los archivos temporales)
CD WINDOWS
DELTREE/Y COOKIES (borra las cookies)
DELTREE/Y TEMP (borra archivos temporales)
DELTREE/Y HISTORY (borra el historial)
DELTREE/Y TEMPOR~1 (borra la caché)
```

Si el último comando no funciona se puede probar:

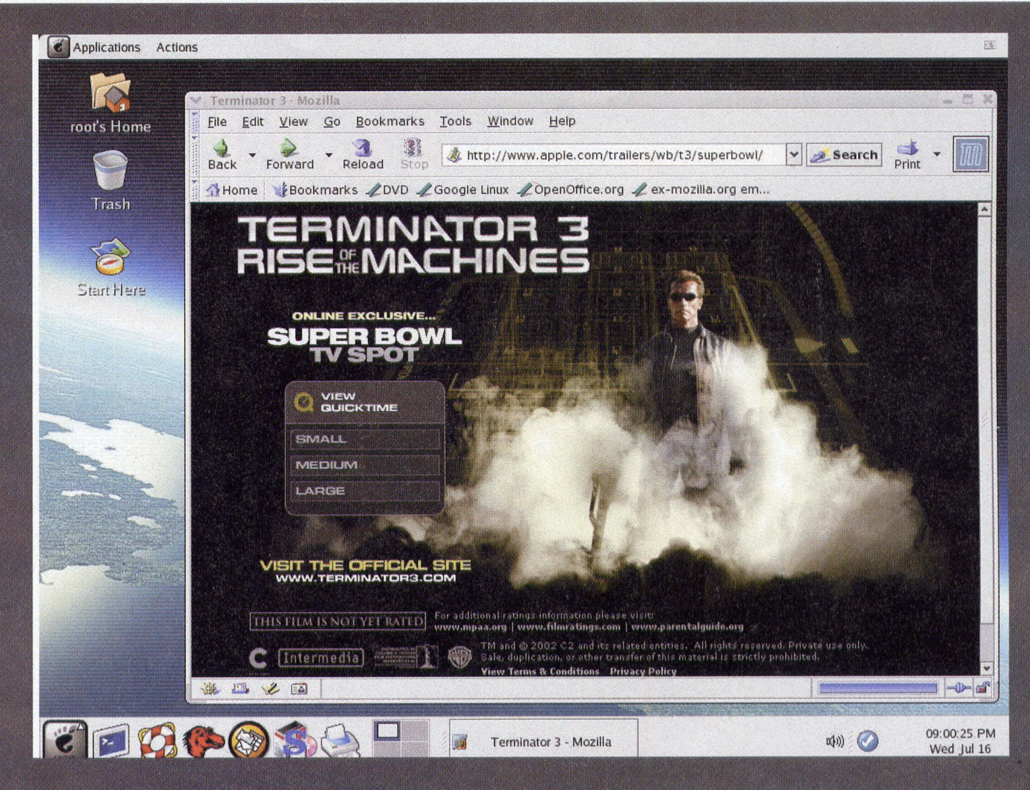
```
CD\WINDOWS\APPLIC~1
DELTREE/Y TEMPOR~1
```

Si esto tampoco funciona, existe otra alternativa:

```
CD\WINDOWS\LOCALS~1
DELTREE/Y TEMPOR~1
```

En caso de problemas, hay que tener en cuenta que algunas versiones de Explorer cambian la posición donde se guardan los datos. Los archivos pueden estar por ejemplo en \windows\profiles\%usuario%\, o en \windows\content\, u otro. Recordemos que en un PC con mucho uso se puede encontrar mucha caché y por ello algunos comandos pueden requerir mucho tiempo. Los comandos de DOS no muestran barra de progreso ni otros indicadores, por lo que no hay que preocuparse si no vemos mensajes del sistema por un tiempo. Tengamos presente que Windows recrea los archivos .dat al reiniciar e por ello no debe extrañarnos que vuelvan a estar ahí. Pero estarán vacíos...





Un secreto banal para no encontrar archivos ocultos en el sistema: usar un navegador distinto de Explorer. Por ejemplo Mozilla.

DIME QUÉ NAVEGADOR USAS

Prácticamente todos los navegadores que no son Internet Explorer son mucho más transparentes e informativos respecto a caché e historial. En Mozilla (http://www.mozilla.org), Opera (http://www.opera.com) y los demás posibles candidatos basta con ejecutar un comando de menú para borrarlo todo inmediatamente.
Explorer es el único que crea datos personales difíciles de encontrar. Conclusión: si no estamos obligados por algo o alguien a usar Explorer, y nos importa la privacidad, usemos otro navegador.

Wine: Windows en

Con un poco de iniciativa y el software adecuado, podemos ejecutar programas para Windows en Linux y tener lo mejor de ambos sistemas



Cuantos programas hay para Windows! Si sólo funcionara algo mejor, costara menos y fuera algo más moderno. Sería un sistema ideal.

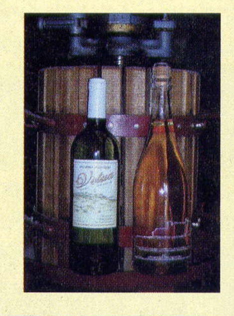
¡Qué gran sistema operativo Linux! Es libre, open source y resuelve un montón de cosas. Es cierto que a veces sería cómodo tener los programas que funcionan bajo Windows. Y resulta que hay un sistema para sacar partido de ambos S.O. a la vez: Wine (http://www.winehq.com).

Técnicamente, Wine es una implementación de las API (Application Programming Interfaces, interfaz para la programación de aplicaciones) de Windows en Unix y en el sistema X (http://www.xfree86.org/). Linux es un sistema basado en Unix y por ello Wine permite que funcionen programas de Windows directamente en un sistema Linux. El software constituye una capa de compatibilidad, no una capa de emulación, lo que significaría prestaciones ridículas.

El código es totalmente Microsoft-free y no requiere poseer Windows. Pero quien tenga Windows puede poner a disposición de Wine DLL nativas, que serán llamadas regularmente. El sistema contiene un toolkit de desarrollo, Winelib, para portar fuentes de Linux a Unix y un program loader, un cargador de programas, para tomar un binario Windows y ejecutarlo directamente, no sólo en Linux sino también en otros sitemas basados en Unix, como FreeBSD o Solaris.

ACRÓNIMOS Y ENTORNOS DE EJECUCIÓN

También el nombre Wine, como GNU, está hecho para ser apreciado por los amantes de la recursividad y los juegos matemáticos. Wine, de hecho, es el acrónimo de Wine Is Not an Emulator (Wine no es un emulador. A propósito, ¿quién sabe decir qué significa GNU?). Aparte de los juegos de palabra, sin embargo, el mensaje es importante. Indica que los programas de Windows no funcionan sobre una capa de emulación; es decir, que Linux no pierde tiempo fingiendo ser Windows y por ello no desperdicia recursos de elaboración. Los programas Windows encuentran las llamadas al sistema que necesitan. Simplemente son llamadas hechas para funcionar bajo Linux.



Instalación (de mayo)

Naturalmente es necesario estar en Linux para usar Wine. Lo primero que hay que hacer es descargar el software de http://www.winehq.com/site/download.

Linux WINE HQ

Se puede descargar el código fuente o bien un archivo binario ya compilado. en el primer caso tenemos que descompactar el software con

```
tar zxvf Wine-AAAAMMGG.tar.gz
```

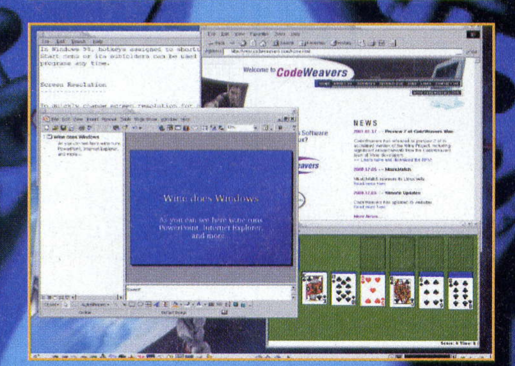
Las versiones de Wine se distinguen por fecha y por ello el comando exacto contiene año, mes y día como aparecen en el nombre del archivo en lugar de las mayúsculas.

Se crea un nuevo directorio. Entramos y escribimos:

```
./configure && make depend && make && su -c "make install"
```

Si en cambio hemos descargado un binario, será un paquete RPM o bien irá acompañado de algún tipo de comando automático. En el primer caso el comando a escribir, como root, es

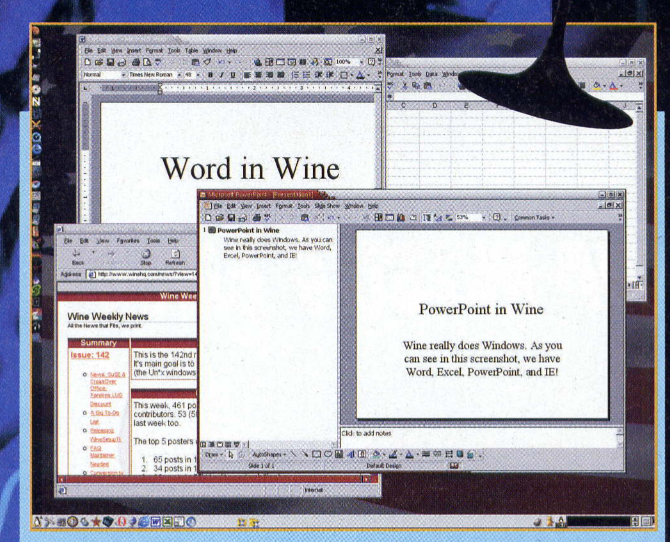
```
rpm -iv wine-AAAAMMGG-i386.rpm
```



↑ *Internet Explorer es uno de los programas de Windows que puede resultar útil hasta en Linux. Con Wine se puede ejecutar.*

En la segunda depende de la distribución y del comando. En Debian, por ejemplo, sería

```
apt-get install wine
```



¿Office en Linux? ¡Es posible!

De mayo 2004 en adelante Wine crea él solo un directorio ~/.wine que contiene todo lo necesario para el funcionamiento general, incluido un falso disco Windows, el mapeado de los discos y todo lo demás. La configuración es prácticamente automática. En compensación se ha conservado el viejo comando wineprefixcreate para quien prefiera hacerlo a su modo.



↑ *No siempre va así de bien, pero muchos juegos de Windows aceptan funcionar con Wine.*

Para asociar un directorio cualquiera a un mapeado Windows se aplica el comando

```
ln -s /mnt/midisco ~/.wine/dosdevices/d:
```

Que mapeará cualquier cosa que corresponda a /mint/midisco en un falso disco Windows d:.
Como siempre, toda la información está contenida en el comando

```
man wine.conf
```

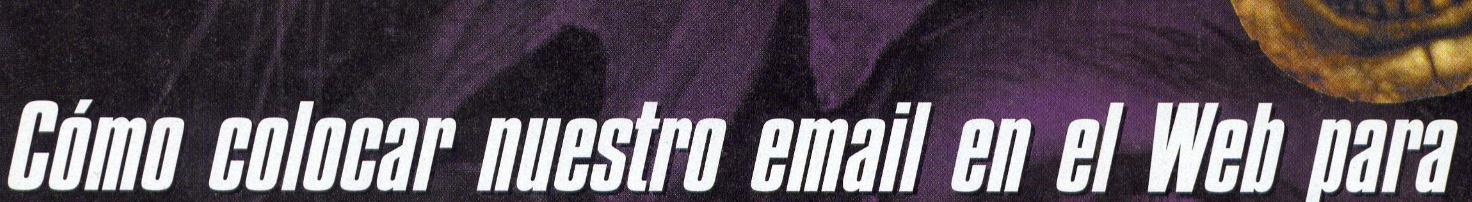
¿Todo claro? ¡Suerte con Wine!



JUNTOS, SIMULTÁNEAMENTE

¿Por qué liarse con Wine cuando se puede particionar con poco esfuerzo el disco duro y tener una partición Windows y una partición Linux? Fácil. El equipo puede usar sólo un sistema operativo a la vez. Si funciona Windows, no se puede tener Linux sin reiniciar y viceversa. Wine es un sistema ingenioso para hacer funcionar los programas de Windows aunque debajo de la manta se encuentra a Linux ocupándose de todo. Elegante, práctico y eficaz. Tras probarlo, cuesta desprenderse de él.

Dirección



Uno de los sistemas más comunes de ocultar nuestro email a los motores de spammer es codificar la dirección como entidad HTML. ¿Es posible que un spambot (los robots de spammer) pueda saber que dentro de la secuencia de caracteres mailto se oculta una vultar dirección mailto...?

El problema es que pensamos demasiado en cómo la vemos nosotros y no tanto en como la ven ellos. El lío de & y # sugiere confusión indescifrable. Además pensamos en los emisores de spam como cretinos, ya que emiten mensajes claramente cretinos. Los mail son cretinos, pero ellos no. Y un spammer comprende pronto cómo están las cosas y estudia una buena expresión regular que capture la entidad HTML. Existe un sistema muy veloz para codificar rápidamente una dirección en entidad (Fantomas MailShield, en la dirección http://fantomaster. com/fantomasSuite/mailShield/famshieldsv-e.cgi), y no es difícil programar la operación inversa.

Si tienes Javascript verás la dirección real. Si no tienes JavaScript verás la dirección Spam Motel, que si eres humano seguirá funcionando, pero si eres un spambot te mantendrá a salvo de correo no deseado

Alguno ha pensado en complicar las cosas, entonces, ocultando (es un decir) la dirección codificada en una entidad dentro de JavaScript, así:

```
<script type="text/javascript">
<!—
document.write('<a href="mail-to:&#109;&#105;&#108;&#097;&#064;&#109;&#097;&#105;&#108;&#046;&#105;&#116;" title="Dirección email codificada.">¡Escríbeme!<\/a>');
// —>
</script>
```

(¿qué dirección, por cierto?) Todo bien, muy astuto, pero hay dos problemas. ¡El primero es que no ha cambiado absolutamente nada para el robot! De hecho la secuencia es la misma, sólo que insertada en un tag (de JavaScript) de más. El spambot lo hallará con una milésima de segundo de retraso, eso es todo. Segundo problema, los links escritos en JavaScript serán evitados. ¡Pocos lo saben, pero más de un usuario no usa JavaScript! Entre los grupos de riesgo están los que usan un navegador de sólo texto, como Lynx (http://lynx.browser.org); los que usan uno normal en la empresa pero por ordenes superiores se ha deshabilitado; y otros muchos.

← *¿Ves qué fácil es convertir una dirección de email en una entidad?*

↑ *Lynx, el navegador de sólo texto, disponible para todos los sistemas operativos del mundo. Cuando no se quieren imágenes, también es el más veloz del mundo. Cargar sólo el HTML, de hecho, es un juego de niños.*



ENMASCARADA

que la lean sólo los humanos. Y que se entienda.



← *Spam Motel (http://www.spammotel.com), el sistema que genera direcciones de email de usar y tirar para combatir al spam.*

Si se usa JavaScript, ya que representa un problema de uso y Web design, al menos bien usado puede poner en verdaderas dificultades a los spambot. Ésta es la idea: unir Javascript y un sistema de direcciones de usar y tirar con el que soltar una cortina de humo a los ojos de los spammer, sin excluir a nadie, ni siquiera a Lynx. El sistema lo tenemos, y está al alcance de todos: es Spam Motel (http://www.spammotel. com). Su mecanismo permite crear todas las direcciones de usar y tirar que queramos y tirarlas cuando reciban spam.

Así, se usa un poco de JavaScript en la sección <head> de las páginas en las que queremos enlazar la dirección de correo, destinado a crear un poco de confusión con la dirección de verdad:

```
<script type="text/javascript">
function ofusca_mail()
{
        mail_inicio =
"mailto:ne0k0n@";
  mail_fin = "urnal.es";
 mail_interno = "hackerjo";
 return mail_inicio + mail_interno
+ mail_fin;
}
</script>
```

Para crear el link propiamente dicho, se combina una dirección de Spam Motel con la función ofusca_mail:

```
<a href="mailto:WGAFJEUYFOQC
@spammotel.com"
onclick="this.href=ofusca_mail();"
onMouseOver="window.status=of
usca_mail();return true;" onmou-
seout="window.status='';return
true;">¡Escríbeme!</a>
```

Aquí viene lo bueno: quien no usa JavaScript, y especialmente un spambot, obtendrá la dirección Spam Motel, que para la persona funcionará pero no para los spammers. Quien usa JavaScript deberá obtener la dirección verdadera, la cual, si se observa, no es visible en el código de la página, a menos que un spambot se ponga a analizar y reducir cadenas encontradas dentro de etiquetas de JavaScript. Son inteligentes, pero no tanto como para llegar hasta esto. ¡Al menos por el momento!
Y tenemos la impresión de que, con el tiempo, se tenderá a revender las direcciones viejas en lugar de crear direcciones nuevas. Con el reciclaje total, es lo más probable...





Máximo SECRETO con KGB

Kgb sirve para ocultar archivos en CDs de audio, de un modo bastante peculiar y naturalmente a prueba de miradas indiscretas

El programa inserta bytes de un archivo que queramos dentro de un archivo .wav que luego masterizamos. El ruido en la canción será mínimo y el programa será capaz de extraer del archivo .wav, transferido del CD al disco duro, nuestro documento oculto. Así es como funciona.

Tenemos no.wav que es una canción y b.zip que es el archivo que queremos ocultar. Bien, copiamos en la misma carpeta también el archivo kgb.exe y entramos en MS-DOS. Lanzamos un simple comando dir para comprender bien la situación:

NO WAV	42.401.927	13/04/02	13.53	no.wav
B ZIP	6.209	03/06/04	11.35	b.zip
KGB EXE	31.075	09/07/04	11.06	kgb.exe

El código de KGB

```
 /*
kgb is a program that can be used to hide
files in music cds.
Coded by witch_blade 09/07/04 11:04:00
www.selphy.tk
www.blackserver.it
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

FILE *wav, *tohide, *final;
char bit[1], bit2[1], byte[1], other[100];

int hide() {

      int a=0;
      long count, c=0;

      printf("Insert the size in byte for the
file to hide:");
      scanf("%d", &count);
      printf("Adding file... please wait...\n");

      for (int b=0; b<44; b++) {
                                    fread(byte, 1,
1, wav);
            fwrite(byte, 1, 1, final);
                                    }

      while (c<count) {
      if (a!=100000) {
                                    fread(bit, 1, 1,
wav);
            fwrite(bit, 1, 1, final);
            a++;
            } else {
            if (count-c>100) {
            fread(other, 100, 1, wav);
            fread(other, 100, 1, tohide);
            fwrite(other, 100, 1, final);
            a=0;
            c=c+100;
            }
            else {
            fread(bit, 1, 1, wav);
            fread(bit2, 1, 1, tohide);
            fwrite(bit2, 1, 1, final);
            a=0;
            c++;
            }
            }
            }

      while (!feof(wav)) {
            fread(bit, 1, 1, wav);
            fwrite(bit, 1, 1, final);
      }

};

int extract() {
      int a=0;
      long count, c=0;
```

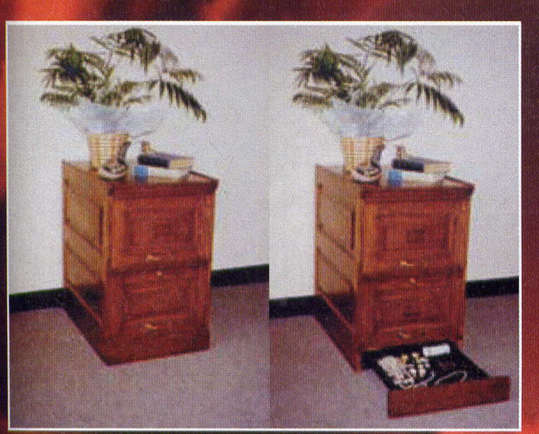
Archivos ocultos en CDs con MÚSICA

Ahora... recordemos que es posible insertar dentro de una canción sólo archivos que sean ligeramente inferiores respecto al tamaño de la canción, en caso contrario se corre el riesgo de provocar errores, de modo que b.zip podría tener hasta 42.000 bytes de tamaño. En este caso son 6.209, por lo que no hay ningún problema y podemos proceder sin interrupciones. Escribimos el comando:

```
kgb -a no.wav b.zip
```

(-a es ADD y no.wav es el archivo wav mientras b.zip es el oculto)

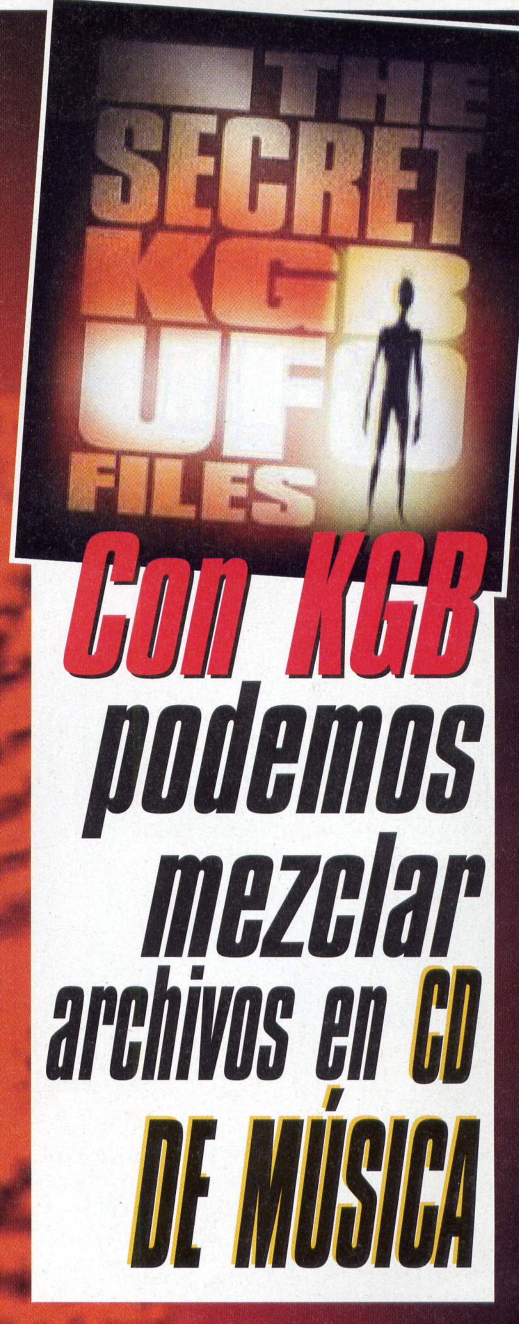
Ahora se pide el tamaño en bytes del archivo b.zip. Este valor se pedirá de nuevo en la fase de extracción y es casi una especie de password, bueno para aumentar el nivel de seguridad. Insertamos el valor 6209 y esperamos un par de minutos. Se crea el archivo kgb.wav listo para ser masterizado.



Es mejor que los viejos métodos de ocultación...

¿Y si ahora queremos extraer el archivo? Simple, basta escribir: kgb -e kgb.wav file.zip
(-e es de EXTRACT, kgb.wav es el archivo contenedor y file.zip es el nombre del archivo a extraer)
Ahora se pide de nuevo el tamaño del archivo y en unas décimas de segundo tendremos nuestro archivo zip.

Quizás este método es para gente paranoica, pero creemos que es interesante darse cuenta de que es posible inocular archivos en otros archivos, sólo con un centenar de líneas en código C, de manera original y seguramente de modo que es difícil pensar que alguien se dé cuenta. ¡Hagamos buen uso de ello!
Os dejamos con el código fuente, de modo que se puedan hacer todas las modificaciones o lo que nos parezca más conveniente. Si hacemos una versión nueva, por favor, dejad el nombre del autor original en su sitio: ¡witch_blade os lo agradecerá!



El código de KGB

```
    printf("Insert the size in byte for the
file to extract:");
    scanf("%d", &count);
     printf("Extracting file... please
wait...\n");

    for (int b=0; b<44; b++) {
                                fread(byte, 1,
1, wav);
                                }

    while (c<count) {
    if (a!=100000) {
                               fread(bit, 1, 1,
wav);
          a++;
          } else {
          if (count-c>100) {
          fread(other, 100, 1, wav);
          fwrite(other, 100, 1, tohide);
          a=0;
          c=c+100;;
          } else {
          fread(bit, 1, 1, wav);
          fwrite(bit, 1, 1, tohide);
          a=0;
          c++;
          }
          }
          }

};

int main(int argc, char *argv[]) {
     if (argc!=4) {
     printf("\nkgb v. 1.0 by witch_blade \n
\
      usage: kgb.exe -[a/e] file.wav
file.ext\n \
        -a : add file to file.wav.\n \
              example: kgb.exe -a file.wav
hide.zip\n\
        -e : extract file from file.wav\n\
              example: kgb.exe -e file.wav
hide.zip\n");
              exit(0);
              }
     if (strcmp(argv[1], "-a")==0) {
               wav = fopen(argv[2], "rb");
              tohide = fopen(argv[3], "rb");
                final = fopen("kgb.wav",
"wb");
              hide();
     } else if (strcmp(argv[1], "-e")==0) {
              wav = fopen(argv[2], "rb");
                tohide = fopen(argv[3],
"wb");
              extract();
     } else {
     printf("\nSyntax error!");
     exit(0);
     }

}
```

Del lenguage al C...

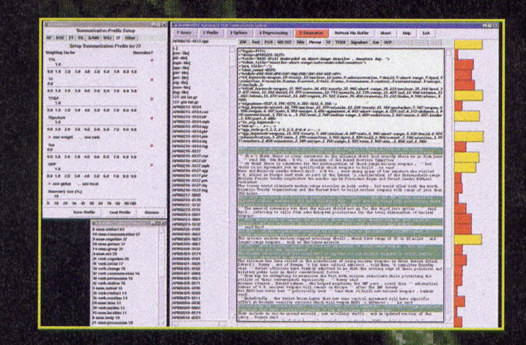
¡Si estamos suficientemente motivados podemos programar cualquier cosa!

Alan Turing explicó en su día que existen problemas que sabemos positivamente que es imposible llegar a resolver, sin importar en absoluto qué ordenador utilicemos para ello.

Kurt Gödel demostró que ningún sistema formal (por ejemplo un lenguaje de programación) está exento de contradicciones internas.

Lo que los programadores pretenden conseguir es realmente sorprendente, como es el traductor de lenguaje C al inglés y viceversa. Se llama c2txt2c, ha sido llevado a cabo por un programador finlandés llamado Leevi Marttila y se puede ver (y descargar) en http://personal.sip.fi/~lm/ c2txt2c.

En los proyectos futuros de Leevi se encuentra la producción de esqueletos diversos, para otras lenguas o bien para dar estilos diferentes a la

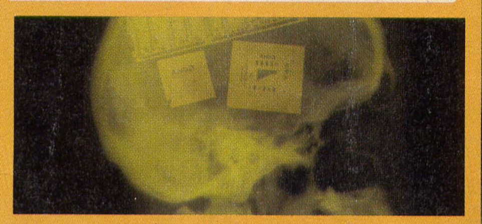


↑ *Un reto difícil para un programa? Traducir un texto y conservar su significado. Para nosotros es algo elemental, sin problemas.*

EL ESQUELETO EN EL DICCIONARIO

El tipo de texto común producido por c2txt2c depende de un esqueleto de lenguaje que se le pasa al programa. A continuación tenéis un ejemplo, que dejamos en inglés para que se aprecie mejor la ambigüedad (¡o la similitud!) entre estructuras de programación y estructuras del lenguaje.

```
for:
{for[s]([expr.1];[expr.2];[expr.3])
[s][compound]} <=>
 {Do next things several times.
Start with this:[s][expr.1]\
  \[s]Does next thing talk about
truth?[s][expr.2]\
  \[s]When you have again done
all, then do this:[s][expr.3]\
  \[s]Here is list of things you
should do:[compound]}
;
```

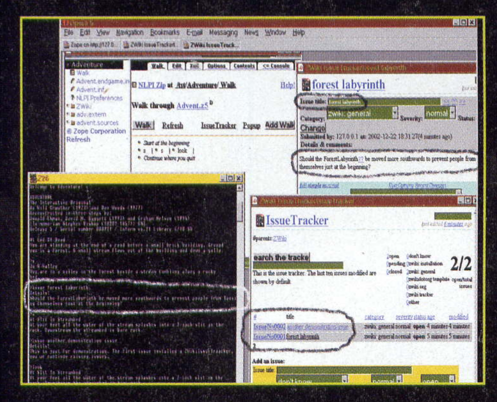


¿Cuántos sueñan con un traductor universal (obviamente en fase de estudio) que simplifique el acercamiento a las bellas muchachas de otros países?





¿Pero a quién se le habría ocurrido jamás un lenguaje que permita hablar con las máquinas igual que uno habla en una cita con las chicas?



↑ *Los programadores de aventuras y juegos en los que se pasan mensajes al programa siempre han necesitado acoplar el lenguaje hablado y el de programación.*

salida, desde humorístico hasta fantástico. De hecho ya está en marcha el trabajo con otros lenguajes de programación para obtener el mismo resultado. Particularmente adaptado, y el primero de todos, es naturalmente Perl. Roger Espel Llima ha realizado ya un primer ejemplo de script, en http://www.iagora.com/~ espel/pleng.

Para estar al corriente existe una mailing list, para inscribirse hay que enviar un mensaje con el asunto subscribe a la dirección de correo lm+c2txt2c-request@sip.fi.

Como se ve en el simple ejemplo que publicamos, la traducción del C al inglés es realmente escolástica. Pero impresiona un poco pensar que, traducido de nuevo del inglés al C, todo el significado del programa queda igual. Seguiremos sus progresos.

...y viceversa

BANANAS, MELONES Y BLOWFISH



Del algoritmo de cifrado Blowfish:

```
/* DCBA - little endian - intel */
#ifdef ORDER_DCBA
union aword {
 UWORD_32bits word;
 UBYTE_08bits byte [4];
 struct {
  unsigned int byte3:8;
  unsigned int byte2:8;
  unsigned int byte1:8;
  unsigned int byte0:8;
 } w;
};
#endif        /* ORDER_DCBA */
```

Traducido en lenguaje natural:

Comment by author: " DCBA - little endian - intel ".
If "ORDER_DCBA" is mentioned, then read next lines.

These briefcases can hold next things:

Treat next things as a compound. There is David code named "word". He likes melons. Move to next person.
There is Thomas code named "byte". Calculate next thing: 4 He likes to carry that amount of bags of cherries. Move to next person.

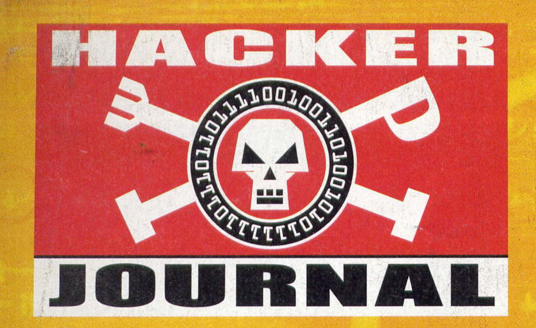
These big chests can hold these things:

Treat next things as a compound. There is Paul code named "byte3". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Eugene code named "byte2". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Wayne code named "byte1". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Joseph code named "byte0". He likes some bananas. His hands are 8 centimeters wide. Move to next person.

Now I have listed all things that belong to that compound. Now George code named "w" is stuffed full.
Now I have listed all things that belong to that compound. However it won't hold those things at the same time.

That was all things related to that thing.





CYBERENIGMA

¡He aquí un nuevo desafío para nuestro Cyberenigma!

A continuación aparece una pregunta; está escrita en un alfabeto muy en boga en el siglo pasado, que nació para aprovechar la invención del telégrafo.

```
-.. . ... -.. .  --.- ..- .  -. .- ...- .  ... .  .-.. .- -. --.. ---  . .-..  .--. .-.
.. -- . .-.  ... --- ...  . -.  -.-. --- -.. .. --. ---  -- --- .-. ... .  -.. .  .-
.. .-  .... .. ... - --- .-. .. .- --..--  .- -. -.. .-. . .-  -.. --- .-. .. .- --..--
.... .. -. -.. . -. -... ..- .-. --. --..--  --.- ..- . . -.  . .-.. .. --.. .- -... . - ....
---  - .. - .- -. .. -.-. .-.-.-  --.- ..- .. . -.  ... . .-  .--. .- .-. - .. -.-. ..-
.-.. .- .-.  -- . -. - .  -.-. ..- .-. .. --- ... ---  .--. ..- . -.. .  .- -.. .. ...- .. -.
.- .-.  .- ... .. -- .. ... -- ---  .-.. .-  ..-. . -.-. .... .- .-.-.-
```

Sintaxis: los espacios separan letras, y dobles espacios separan palabras.

✪ Para todos: ¿de qué alfabeto se trata?
✪✪ Para expertos: ¿Qué dice la pregunta?
✪✪✪ Para genios: ¿Cuál es la respuesta correcta?
✪✪✪✪ Para súper hackers: ¿Quién se atreve a escribir un programa de traducción automática de este alfabeto al nuestro, e incluso al revés?

Para desesperados:
En Internet se encuentran motores ya hechos, que traducen en uno u otro sentido. Quien necesite ayuda puede probar una búsqueda en un buscador como Goggle. Probad por ejemplo a buscar "morse traductor". Pero recordad que el verdadero hacker disfruta resolviendo por sí solo el problema.

Hasta la próxima